VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

KATEDRA APLIKOVANÉ INFORMATIKY

Implementace řízení dostupnosti IT služeb dle ITIL

Availability Management Implementation of IT Services by ITIL

Student: Bc. Vladimír Spál

Vedoucí diplomové práce: Ing. Jan Ministr, Ph.D.

Ostrava 2010

Rád bych poděkoval Ing. Janu Ministrovi, Ph.D. a zástupcům společnosti *Crux information technology, s.r.o.* za odbornou pomoc a profesionální přístup při vedení této diplomové práce.

„Místopřísežně prohlašuji, že jsem celou diplomovou práci včetně příloh vypracoval samostatně.“

V Ostravě dne 30. dubna 2010 ……

Bc. Vladimír Spál

Obsah

1 Úvod

Stále častejšie zisťujeme, že informácie sú najdôležitejší strategický zdroj, ktorý musí každá organizácia riadiť. Kľúčom k zberu, analýze, výrobe a distribúcii informácií v rámci organizácie je kvalita IT služieb poskytovaných podniku. Je podstatné, aby sme si uvedomili, že IT služby sú zásadné strategické organizačné aktíva a preto musia organizácie investovať potrebné množstvo zdrojov na podporu, realizáciu a riadenie týchto zásadných IT služieb a IT systémov, ktoré sú ich oporou. Avšak v mnohých organizáciách sú tieto aspekty IT často prehliadané alebo sú riešené len povrchne. [3]

Primárnym cieľom riadenia služieb je zabezpečiť, aby IT služby boli v súlade s podnikovými potrebami a aktívne ich podporovali. Pre všetky organizácie, ktoré používajú IT, je IT dôležitou súčasťou úspechu. Ak sú procesy a IT služby implementované, riadené a podporované vhodným spôsobom, podnikanie bude úspešnejšie, znížia sa náklady, zvýšia sa príjmy, zlepšia sa vzťahy s verejnosťou a obchodné ciele budú dosiahnuté. [3]

ITIL je verejný rámec, ktorý opisuje Best Practice postupy v oblasti riadenia IT služieb. Poskytuje rámec pre riadenie IT služieb a zameriava sa na neustále meranie a zlepšovanie kvality IT služieb poskytovaných tak z podnikovej, ako aj zákazníckej perspektívy. Toto zameranie je hlavným faktorom úspechu ITIL po celom svete a prispelo k jej produktívnemu využitiu a ku kľúčovým výhodám získaným týmito organizáciami nasadením techník a procesov ITIL vo všetkých častiach ich organizácií. [3]

Aj v Českej republike sa začína presadzovať ITIL nielen vo veľkých organizáciách, ale aj v malých a stredných. Pokiaľ sa organizácie rozhodnú implementovať ITIL, nie je nutné, aby ju implementovali celú. Najmä malé a stredné firmy využívajú iba jej jednotlivé časti a aplikujú ich na oblasti IT, ktoré chcú zlepšiť alebo na tie, ktoré vidia ako problematické. Na problémy, s ktorými sa firmy stretávajú, už pravdepodobne pred nimi narazili iné firmy a ITIL obsahuje ich riešenia, pretože ITIL vznikla zberom skúseností úspešných firiem, ktoré už našli spôsob, ako rýchlo určovať dopady zmien na infraštruktúru a ako riadiť vzťahy s biznisom. ITIL teda ponúka znalosti, s ktorými stojí za to sa zoznámiť a ušetriť si tým niektoré nepríjemné skúsenosti a náročné hľadanie riešení. [17]

Malé a stredné firmy najčastejšie začínajú pri implementácii ITIL užívateľskou podporou, teda manažmentom incidentov. Existuje preň mnoho freewarových riešení a rýchlo nastáva viditeľná zmena vo vzťahu IT - užívateľ. Pokračujú ďalšími, povedzme základnými, ITIL procesmi, ako sú manažment problémov, zmien, úrovní služieb a konfiguračný manažment.

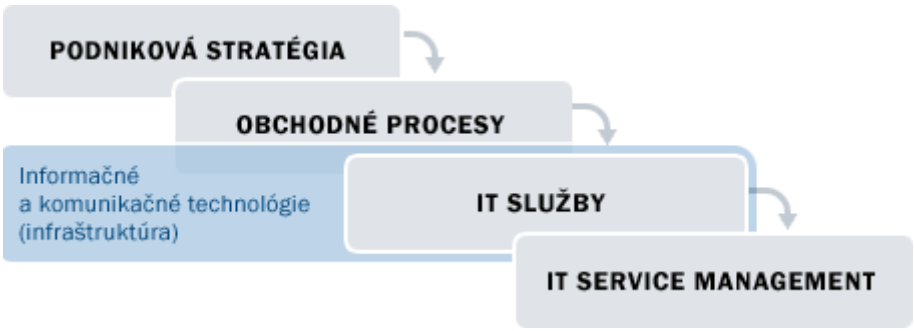
Pokiaľ chcú manažment IT služieb v ich organizácii dostať na ešte vyšší stupeň, prichádza na rad obvykle implementácia procesu manažment dostupnosti. Dostupnosť je u IT služieb najčastejšie subjektívne posudzovaný kvalitatívny ukazovateľ, ale firmy ho len zriedkavo vedia uchopiť a merať. Je rozšíreným mýtom, že všetko musí fungovať 24 hodín 365 dní v roku pri plnení najvyšších záruk. Pritom IT na to mnohokrát nemá zdroje a je to tiež neefektívne, pretože táto predstava nevychádza z reálnych potrieb biznisu. Preto som sa po dohode so zástupcami spoločnosti Crux information technology, s.r.o. rozhodol pre tému mojej diplomovej práce, ktorou je implementácia manažmentu dostupnosti IT služieb podľa ITIL. Cieľom mojej diplomovej práce je vytvoriť návrh metodologickej príručky, ktorá sa bude venovať návrhu postupu implementácie manažmentu dostupnosti IT služieb v malých a stredných firmách.

2 Teoretické východiská manažmentu dostupnosti IT služieb

2.1 ITIL

ITIL (IT Infrastructure Library) poskytuje rámec Best Practice doporučení pre riadenie IT služieb (ITSM, IT Service Management) a od doby svojho vzniku sa ITIL rozrástla na najuznávanejší prístup k ITSM na svete. [3]

2.1.1 ITSM



Obr. 2.1 Zaradenie IT služieb (zdroj [9])

Čo sú to IT služby a prečo je potrebné zaoberať sa ich riadením vyplýva z obrázku 2.1. Zmysel existencie každého podniku je daný jeho podnikovou stratégiou, ktorá okrem iného definuje, čo je predmetom jeho podnikania, akými činnosťami sa podnik zaoberá, ako je organizovaný a riadený, aké sú jeho ciele napríklad v oblasti marketingu, výroby, financií atď. Podniková stratégia následne určuje podobu obchodných procesov, ktoré musia v podniku existovať na to, aby pomocou nich mohol podnik dosiahnuť svoje ciele, ktoré sú určené podnikovou stratégiou. [3], [9]

Podnikové procesy v dnešnej dobe potrebujú pre svoje zmysluplné fungovanie služby informačných a komunikačných technológií. Tieto služby skrátene nazývame IT službami. Všetky IT služby samozrejme fungujú na určitej IT infraštruktúre, ktorá je vždy určitým spôsobom riadená. Obvykle je za jej riadenie zodpovedný úsek informačných a komunikačných služieb, ktorý sa stará o jednotlivé komponenty infraštruktúry. [3], [9]

Aj keď riadenie samotnej technickej a technologickej podstaty IT infraštruktúry je nevyhnutnou podmienkou správneho fungovania IT služieb, nie je podmienkou dostačujúcou. Je totiž potrebné tiež určitým spôsobom riadiť aj samotné IT služby, kvôli ktorým táto infraštruktúra existuje. Toto riadenie sa nazýva IT Service Management. [3]

2.1.2 Vývoj ITIL

Začiatkom 80. rokov sa vo svete objavuje nový špecifický problém a tým je narastajúca závislosť na ICT technológiách a z toho vyplývajúci rast požiadaviek na kvalitu IT služieb. Britská vláda poverila CCTA (Central Computer and Telecommunications Agency) spracovaním príručky, podľa ktorej by organizácie participujúce na dodávkach IT služieb pre britskú vládu museli záväzne postupovať. Vzniká ITIL vo verzii 1. CCTA postupne vydáva 46 zväzkov zhrňujúcich Best Practices z oblasti riadenia IT služieb a infraštruktúry pre potreby britských vládnych úradov a podnikateľských subjektov dodávajúcich IT služby vláde. [3], [10]

Začiatkom 90. rokov vzniká OGC (Office of Government Commerce) zlúčením troch britských vládnych agentúr, vrátane CCTA, a stáva sa autoritou pre re-edície a vydávanie ďalších publikácií ITIL. Vzniká itSMF (IT Service Management Forum) a stáva sa medzinárodnou komunitou profesionálov a odbornej verejnosti z oblasti ITSM a ITIL. Rámec ITIL preberajú ďalšie subjekty súkromného i verejného sektoru. Začína vydávanie prvých certifikátov odbornej spôsobilosti pre oblasť ITSM podľa ITIL. [3], [10]

Na prelome storočí vzniká ITIL vo verzii 2. Pôvodných 46 zväzkov knižnice je prepracovaných do podoby, keď základ knižnice tvoria tituly Service Support a Service Delivery, ktoré obsahujú podstatnú časť z pôvodných 46 zväzkov a v podstate definujú oblasť ITSM. Sú vydávané ďalšie diely knižnice a ITIL je celosvetovo rozšírený a vďaka tomu je považovaný za medzinárodný štandard v oblasti ITSM a prakticky sa už stáva samostatným odborom činnosti a podnikania. [3], [10]

V novembri 2004 OGC zahajuje práce už na tretej aktualizácii knižnice ITIL. V decembri 2005 je zverejnená medzinárodná norma pre oblasť ITSM - ISO/IEC 20000. V máji 2007 vychádza očakávaná ITIL verzia 3. [3], [10]

2.1.3 ITIL V3

Päť hlavných kníh týkajúcich sa životného cyklu služby spolu s oficiálnym úvodom (šiesta kniha) tvoria východiskový bod pre ITIL V3. Týchto päť hlavných kníh pokrýva vlastne každú etapu životného cyklu služby, ako môžete vidieť na obrázku 2.2. [3]

1. **Stratégia služieb (Service Strategy).** V prvej fáze životného cyklu prebieha výber služby, ktorú bude organizácia poskytovať. Vyberie sa taká služba, ktorá prinesie zisk a oplatí sa ju prevádzkovať. [17]

Obr. 2.2 Životný cyklus služby (zdroj <http://www.redengineconsulting.com>)

2. **Návrh služieb (Service Design).** Tu sa navrhuje, ako bude vybraná služba vypadať a z akých technológií sa bude skladať. Návrhy sú dokumentované tak, aby bolo možné službu implementovať, prevádzkovať a zlepšovať. [17]

3. **Prechod služieb (Service Transition).** V tejto fáze je navrhnutá služba fyzicky vytvorená (napr. že je naprogramovaná alebo že je zakúpený HW). Úlohou fáze prechod služby je potom na základe balíčku návrhu služby (SDP) nasadiť službu do prevádzky tak, aby ju užívatelia mohli začať využívať. [17]

4. **Prevádzka služieb (Service Operation).** V rámci fáze Service Operation je služba prevádzkovaná a podlieha bežnej podpore IT. [17]

5. **Neustále zlepšovanie služieb (Continual Service Improvement).** Jednu knihu ITIL venuje práve meraniu a zlepšovaniu služieb. Zlepšovanie je realizované priebežným monitorovaním a meraním procesov, služieb a infraštruktúry a vyhľadávaním príležitostí pre zvyšovanie kvality a znižovanie nákladov. Hlavným procesom je 7-Step Improvement Process. [17]

2.1.4 Rozdiely medzi ITIL V2 a V3

Najväčšou zmenou v ITIL V3 na rozdiel od verzie 2 je sledovanie celého životného cyklu IT služby. Tento cyklus som už predstavil v predchádzajúcej časti. Už od nástupu verzie 2 na trh sa začali práce na verzii 3, ktoré sa zamerali najmä na doplnenie niektorých oblastí. Potreba doplnenia vznikla najmä preto, lebo ITIL V2 vznikala v dobe, kedy úloha IT bola odlišná od dnešnej. Postupom času sa zmenili výzvy, ktorým IT oddelenia čelia.

Z toho vyplýva, že pôvodne bola ITIL viac zameraná na internú prevádzku a procesy, na rozdiel od novej verzie, ktorá je zameraná na stratégiu, služby a zákazníkov. [8], [18]

Spomínané doplnené oblasti sa dajú zhrnúť do štyroch bodov:

- **ITIL je doplnená o stratégiu služieb.** Procesy a techniky stratégie služieb majú zaistiť, aby celé úsilie spojené s prevádzkovaním IT služieb bolo namierené správnym smerom. Stratégia služieb pomáha odpovedať na otázky: Do akých služieb investujeme svoje zdroje? Čo tieto služby prinesú zákazníkovi? Ako sa odlíšime od konkurencie? Poskytuje nám návod, ako z IT vytvoriť strategickú jednotku, ktorá priamo a výrazne pôsobí na výkon firmy a umožňuje jej predbehnúť a odlíšiť sa od konkurencie. Ide o to nerobiť len veci správne, ale aj robiť tie správne veci. [18]
- **Riadené sú nielen procesy, ale aj služba.** ITIL V3 se nezameriava len na procesy, ale hlavne na ich výstupy, čiže služby. K riadeniu procesov, funkcií a ostatných aspektov IT pristupuje z pohľadu služby a koncového užívateľa. Zohľadňuje životný cyklus služby, teda jej strategické umiestnenie (rozhodnutia komu a ako ju poskytovať, jej návrh, zavedenie do prevádzky, prevádzka a zlepšovanie). Všetky hlavné procesy a aktivity ITIL sú začlenené do tohto životného cyklu a tým je zdôraznené, ako prispievajú k dodávke služby zákazníkovi. [18]
- **Sú doplnené ďalšie chýbajúce oblasti.** Vo verzii 3 sú stanovené pravidlá pre zrušenie služieb, ktoré v 2 chýbali. Ďalšie oblasti, ktoré pôvodne chýbali, sú správa dodávateľov a výber sourcingových stratégií. Vo fáze prechod služieb ITIL V3 prichádza s novinkou, počiatočnou podporou (Early life Support) a vo fáze prevádzka služieb s plnením požiadaviek (Request Fulfillment) a so správou udalostí (Event Management). Tiež sa viac venuje ľudskej stránke nasadzovania procesov a zavádzania zmien. Využívajú sa na to psychologické poznatky, napríklad tzv. emočný cyklus zmeny. [17], [18]
- **Zosúladenie IT a biznisu.** Dôraz je kladený na hľadanie rovnováhy v rôznych oblastiach prevádzkovania IT služieb. Ide o to, že IT oddelenie by sa malo riadiť potrebami biznisu, ale nesmie to byť na úkor jeho stability a zdravia. Je potrené dosiahnuť rovnováhu medzi stabilitou a flexibilitou. Tiež je tu riešená otázka pro-aktívneho a reaktívneho prístupu. [18]

Rozdiely v kľúčových procesoch ITIL V2 a ITIL V3 sú popísané v tabuľke, ktorú som umiestnil do príloh pod označením A.

2.2 Manažment dostupnosti

Manažment dostupnosti je jeden z kľúčových procesov ITIL. Vo verzii 2 je zaradený v rámci Service Delivery a v 3 v rámci Service Design. Práve tieto dve knihy som použil na vypracovanie tejto teoretickej časti mojej diplomovej práce. V použitej literatúre sú uvedené pod označením [4] a [5].

2.2.1 Ciele manažmentu dostupnosti

Cieľom procesu manažment dostupnosti je postarať sa o to, aby úroveň dostupnosti služieb v rámci všetkých služieb spĺňala alebo presahovala dohodnuté súčasné a budúce podnikové potreby, a aby to bolo dosiahnuté nákladovo efektívnym spôsobom. Účelom manažmentu dostupnosti je riadiť a sústrediť sa na otázky spojené s dostupnosťou, týkajúce sa služieb a zdrojov, a taktiež zabezpečiť, aby všetky ciele v oblasti dostupnosti boli merané a dosiahnuté.

Ciele manažmentu dostupnosti sú:

- Vypracovať a udržiavať prijateľný a aktuálny plán dostupnosti, ktorý odráža súčasné a budúce potreby podniku;
- Poskytnúť radu a poučenie všetkým častiam podniku a IT vo všetkých otázkach týkajúcich sa dostupnosti;
- Zabezpečiť, aby dosiahnuté výsledky v oblasti dostupnosti služieb dosiahli či presiahli dohodnuté ciele, a to riadením služieb a so zdrojmi súvisiaceho výkonu dostupnosti;
- Pomáhať s diagnostikou a riešením problémov a incidentov týkajúcich sa dostupnosti;
- Hodnotiť dopady všetkých zmien na plán dostupnosti a na výkon a kapacitu všetkých služieb a zdrojov;
- Zabezpečiť, aby boli zrealizované pro-aktívne opatrenia na zlepšenie dostupnosti služieb kdekoľvek, kde je to nákladovo oprávnené.

Riadenie dostupnosti by malo zabezpečiť, že je poskytovaná dohodnutá úroveň dostupnosti. Meranie a sledovanie dostupnosti IT je kľúčom k trvalému dosahovaniu vyžadovanej úrovne dostupnosti. Manažment dostupnosti by sa mal neustále sústrediť na optimalizáciu a zlepšovanie dostupnosti IT infraštruktúry a služieb za účelom poskytnutia nákladovo efektívneho zvýšenia dostupnosti, ktoré by poskytlo výhody podniku aj zákazníkom.

2.2.2 Rozsah manažmentu dostupnosti

Rozsah procesu manažment dostupnosti zahŕňa návrh, implementáciu, meranie a zlepšovanie dostupnosti IT služieb a komponentov. Manažment dostupnosti musí porozumieť požiadavkám na dostupnosť služieb a komponentov z obchodného hľadiska: súčasným podnikovým procesom, ich fungovaniu a požiadavkám; budúcim podnikovým plánom a požiadavkám; cieľom v oblasti služieb, fungovaniu a doručovaniu súčasných IT služieb, IT infraštruktúre, dátam, aplikáciám, prostrediu a ich výkonu; dopadom na podnik a prioritám vo vzťahu k službám a ich využívaniu. Pochopenie tohto všetkého pomôže manažmentu dostupnosti dosiahnuť, aby všetky služby a ich komponenty boli navrhnuté a doručené tak, aby dosiahli určené ciele v rámci dohodnutých odchodných podmienok.

Proces riadenia dostupnosti:

- by sa mal aplikovať na všetky prevádzkované služby a technológie, najmä tie, ktoré sú zahrnuté v SLA[1], môžu sa tiež aplikovať aj na tie služby, ktoré sú pre podnik veľmi dôležité, hoci nie sú zahrnuté v SLA;
- by sa mal aplikovať na všetky nové IT služby a na tie už existujúce, pre ktoré boli stanovené SLA a SLR[2];
- by sa mal aplikovať na podporné služby, na partnerov a dodávateľov (ako interných, tak externých), ktorí formujú IT podpornú organizáciu ako predzvesť vytvorenia formálnych dohôd;
- zvažuje všetky aspekty IT služieb, komponentov a podporných organizácií, ktoré môžu mať dopad na dostupnosť, vrátane školenia, zručností, efektívnosti procesov, procedúr a nástrojov.

Proces riadenia dostupnosti nezahŕňa riadenie obchodnej kontinuity (BCM, Bussines Continuity Management) a obnovenie podnikových procesov po veľkej katastrofe. Podpora BCM je súčasťou IT Service Continuity Management[3] (ITSCM). Avšak riadenie dostupnosti poskytuje kľúčové vstupy do ITSCM, a tieto dva procesy majú blízky vzťah, obzvlášť v oblasti hodnotenia a riadenia rizík, implementácie opatrení na zníženie rizík a zvýšenie odolnosti. Proces riadenia dostupnosti by mal zahŕňať:

---

[1] Service Level Agreement, Dohoda o úrovni služby medzi poskytovateľom IT služieb a zákazníkom. SLA popisuje IT službu, dokumentuje cieľovú úroveň služieb a špecifikuje zodpovednosti poskytovateľa IT služby a zákazníka. [13]

[2] Service Level Requirement, Požiadavky na úroveň služby. Požiadavka zákazníka na stav IT služby. [13]

[3] Manažment kontinuity IT služieb. Proces zodpovedný za manažment rizík, ktoré môžu mať vážny dopad na IT služby. [13]

- Všetky aspekty dostupnosti, spoľahlivosti a udržateľnosti IT služieb a podporných komponentov, s prijateľnými udalosťami, alarmami a stupňovaním, s automatickými scenármi na ozdravenie;
- Údržba rady metód, techník a výpočtov pre všetky merania, veličiny a hlásenia dostupnosti;
- Asistencia s meraním rizík a riadiacimi aktivitami;
- Zbierka meraní, analýzy a produkovanie pravidelných a prípadových správ o dostupnosti služieb a komponentov;
- Porozumenie dohodnutému súčasnému a budúcemu dopytu podniku po IT službách a ich dostupnosti;
- Ovplyvňovanie návrhu služieb a komponentov, aby boli v súlade s podnikovými potrebami;
- Vytvorenie plánu dostupnosti, ktorý umožní poskytovateľovi služieb pokračovať v poskytovaní a zlepšovaní služieb v súlade s cieľmi týkajúcimi sa dostupnosti dohodnutými v SLA, a plánovať a predvídať budúce vyžadované úrovne dostupnosti tak, ako sa dohodli v SLR;
- Udržiavať rozvrh testov pre všetky zlyhaniu odolávajúce komponenty a mechanizmy;
- Asistovať s identifikáciou a riešením problémov a incidentov spojených s nedostupnosťou služieb či komponentov;
- Pro-aktívne zlepšovanie služieb a komponentov, kdekoľvek je to v súlade so záujmami podniku, a kde je to nákladovo oprávnené.

2.2.3 Politiky, prístupy a základné koncepty

Proces riadenia dostupnosti zaisťuje, aby všetky prevádzkované služby spĺňali dohodnuté ciele dostupnosti, a aby nové služby a komponenty boli vhodne navrhnuté na dosahovanie plánovaných cieľov. V záujme toho musí riadenie dostupnosti rozvíjať reaktívne aj pro-aktívne aktivity.

- **Reaktívne aktivity**: reaktívny aspekt riadenia dostupnosti zahŕňa sledovanie, meranie, analyzovanie a riadenie všetkých udalostí, incidentov a nehôd týkajúcich sa nedostupnosti. Tieto aktivity sú v prvom rade súčasťou operačných úloh.
- **Pro-aktívne aktivity**: pro-aktívne riadenie dostupnosti zahŕňa pro-aktívne plánovanie, návrh a zlepšovanie dostupnosti. Tieto aktivity sú hlavne súčasťou úloh v oblasti plánovania a projektovania.

Existuje niekoľko vedúcich princípov, ktoré by mali byť opornou kostrou procesu riadenia dostupnosti a jeho hlavným predmetom:

- Dostupnosť služieb je jadrom spokojnosti zákazníkov a podnikového úspechu. Existuje priama korelácia medzi dostupnosťou služieb a spokojnosťou zákazníkov a užívateľov vo väčšine takých podnikov, kde sa slabá výkonnosť služieb definuje ako nedostupnosť služieb.
- Uvedomiť si, že aj keď služba zlyhá, je možné dosiahnuť spokojnosť podniku, užívateľov a zákazníkov a pochopiť, že spôsob, akým poskytovateľ služieb reaguje v prípade zlyhania, má veľký vplyv na očakávania a dojem zákazníkov a užívateľov.
- Zlepšiť dostupnosť je možné až po pochopení, ako IT služby podporujú fungovanie podniku.
- Celková dostupnosť služieb je iba taká dobrá, ako je najslabší článok reťaze. Je možné ju vo veľkej miere zvýšiť jednoduchým odstránením jednotných zdrojov zlyhania (SPOF[4]), prípadne nespoľahlivého či slabého komponentu.
- Dostupnosť nie je len reaktívnym procesom. Čím je proces aktívnejší, tým je dostupnosť lepšia. Dostupnosť by nemala len reagovať na zlyhania služieb či ich komponentov. Čím viac sú podobné situácie a zlyhania očakávané, čím viac sa im zabraňuje a predchádza, tým je úroveň dostupnosti vyššia.
- Je lacnejšie navrhnúť správnu úroveň dostupnosti služby od jej začiatku, než sa ju tam snažiť následne vmontovať. Pridávanie aspektov odolnosti do služieb je nevyhnutne oveľa nákladnejšie, než keď je odolnosť súčasťou návrhu od samého počiatku. Takisto, ak raz utrpí dobrá povesť služby kvôli nespoľahlivosti, je len veľmi ťažké tento dojem zmeniť. Odolnosť je tiež kľúčovým faktorom pre ITSCM, čo by sa tiež malo vziať do úvahy.

Riadenie dostupnosti je zavŕšené na dvoch navzájom prepojených úrovniach:

- **Dostupnosť služby**: zahŕňa všetky aspekty dostupnosti aj nedostupnosti služieb a vplyv dostupnosti komponentu, prípadne možný dopad nedostupnosti komponentu na nedostupnosť služby.
- **Dostupnosť komponentov**: zahŕňa všetky aspekty dostupnosti a nedostupnosti komponentov.

[4] Single Point of Failure, je každá konfiguračná položka, ktorá môže zapríčiniť incident, keď zlyhá, a pre ktorú nebolo implementované protiopatrenie. SPOF môže byť rovnako osoba alebo krok v procese alebo aktivite ako aj komponent IT infraštruktúry. [13]

Manažment dostupnosti sa spolieha na meranie, sledovanie, analyzovanie a hlásenie nasledujúcich aspektov:

- **Dostupnosť**: schopnosť služby, komponentu alebo CI[5] vykonať funkciu, keď sa to vyžaduje. Často sa meria a vyjadruje ako percentuálna hodnota.

$$Dostupnosť(\%) = \frac{(dohodnutý\ čas\ trvania\ služby - prestoje)}{dohodnutý\ čas\ trvania\ služby} \times 100 \quad (1)$$

(prestoje by mal byť zahrnuté do výpočtu, iba ak sa objavia počas dohodnutého času trvania služby)

(zdroj [5])

- **Spoľahlivosť**: meranie toho, ako dlho služba, komponent či CI dokážu vykonávať dohodnutú funkciu bez prerušenia. Spoľahlivosť služby je možné zvýšiť zvýšenou spoľahlivosťou jej komponentov alebo zväčšením jej odolnosti voči zlyhaniu jej jednotlivých komponentov (napr. zvýšiť nadbytočnosť komponentov, využitím techník vyrovnávajúcich záťaž). Často sa meria a vyjadruje ako priemerný čas medzi výskytom incidentov služieb (MTBSI[6]) a priemerný čas medzi výskytom zlyhaní (MTBF[7]).

$$Spoľahlivosť\ (MTBSI\ v\ hodinách) = \frac{dostupný\ čas\ v\ hodinách}{počet\ prerušení} \quad (2)$$

$$Spoľahlivosť\ (MTBF\ v\ hodinách) = \frac{\left(\begin{array}{c} celkový\ čas\ k\ dispozícii\ v\ hodinách \\ - celkové\ prestoje\ v\ hodinách \end{array}\right)}{počet\ prerušení} \quad (3)$$

(zdroj [5])

- **Udržateľnosť**: meranie toho, ako rýchlo a efektívne je možné službu, komponent či CI navrátiť po zlyhaní do normálnej prevádzky. Vyjadruje sa a meria ako priemerný čas znovuobnovenia služby (MTRS[8]).

$$Udržateľnosť\ (MTRS\ v\ hodinách) = \frac{celkové\ prestoje\ v\ hodinách}{počet\ servisných\ prestávok} \quad (4)$$

(zdroj [5])

Prestoje v MTRS zahŕňajú všetky faktory, ktoré majú podiel na tom, že služba nie je dostupná: čas na zaznamenanie, čas na reakciu, čas na vyriešenie problému, čas

[5] Configuration Item, konfiguračná položka. Akýkoľvek komponent, ktorý je potrebné manažovať za účelom dodávky IT služby.
[6] Mean Time Between Service Incidents
[7] Mean Time Between Failures
[8] Mean Time to Restore Service

na fyzickú opravu či nahradenie, čas vrátiť sa do pôvodnej pozície, čas na ozdravenie, čas dostať sa z ťažkostí.

- **Servisovateľnosť (schopnosť poskytovať službu)**: schopnosť tretej strany (dodávateľa) dodržať podmienky zmluvy. Najčastejšie zmluva obsahuje dohodnuté úrovne dostupnosti, spoľahlivosti a udržateľnosti podpornej služby či komponentu.

Hoci najdôležitejším cieľom v oblasti služieb zahrnutých v SLA je dostupnosť, niektorí zákazníci vyžadujú, aby ciele v oblasti spoľahlivosti a udržateľnosti boli takisto zahrnuté.

Pojem životne dôležitá funkcia podniku (VBF[9]) sa používa na označenie kritických podnikových elementov v rámci podnikových procesov podporovaných IT službou. IT služba môže podporovať celý rad podnikových funkcií, ktoré sú menej zásadné. Napríklad, u bankomatu by bolo životnou funkciou vydávanie peňazí. Avšak možnosť získať výpis z účtu nemusí byť nutne považovaná za životne dôležitú. Toto rozlíšenie je dôležité a malo by ovplyvniť návrh dostupnosti a s tým spojené náklady. Vo všeobecnosti platí, že čím ide o dôležitejšiu podnikovú funkciu, tým väčšiu odolnosť a dostupnosť je nutné požadovať v návrhu na podporu IT služieb. Pre všetky služby platí, či už ide o životne dôležité funkcie podniku alebo nie, že požiadavky na dostupnosť by mal formulovať podnik, nie IT. Počiatočné ciele v oblasti dostupnosti sú zvyčajne stanovené príliš vysoko, a to vedie buď k premršteniu ceny za služby, alebo to vedie k opakovaným diskusiám medzi podnikom a poskytovateľom služby s cieľom dohodnúť sa na vhodnom kompromise medzi dostupnosťou služby a nákladmi spojenými so službou a podpornými technológiami.

Riadenie dostupnosti je zahájené v okamihu, keď sú požiadavky na dostupnosť IT služieb na toľko jasné, aby mohli byť formulované. Jedná sa o neprerušený proces, ktorý je ukončený až v okamihu, keď je IT služba vyradená z prevádzky alebo úplne ukončená. Kľúčovými aktivitami manažmentu dostupnosti sú:

- určenie požiadaviek dostupnosti na novú alebo vylepšenú IT službu podnikom a formulovanie konštrukčných kritérií pre dostupnosť a ozdravenie podporných IT komponentov;
- určenie životne dôležitých funkcií podniku, v spojení s podnikom a ITSCM;
- určenie dopadu zlyhania IT služby alebo komponentov v spojení s ITSCM a tam, kde je to potrebné, prehodnotiť návrhové kritériá na dostupnosť za účelom poskytnutia dodatočnej odolnosti, a tak zabrániť alebo znížiť dopad na podnik;

[9] Vital Business Function

- definovať ciele v oblasti dostupnosti, spoľahlivosti a udržateľnosti pre komponenty IT infraštruktúry, ktoré podporujú IT služby, aby tie mohli byť zdokumentované a dohodnuté v SLA, OLA[10] a zmluvách;
- vytvorenie meraní a podávanie hlásení o dostupnosti, spoľahlivosti a udržateľnosti, ktoré odrážajú perspektívu podniku, užívateľa a IT podpornej organizácie;
- sledovanie a trendové analýzy dostupnosti, spoľahlivosti a udržateľnosti IT komponentov;
- kontrola dostupnosti IT služieb a komponentov a identifikácia neprijateľných úrovní;
- vyšetrovanie zásadných dôvodov neprijateľnej dostupnosti;
- vytvorenie a udržiavanie plánu dostupnosti, ktorý určuje priority a plánuje vylepšenia dostupnosti IT.

Kľúčové rozhrania, ktoré má manažment dostupnosti s inými procesmi, sú:

- Incident a problém manažment: pri poskytovaní pomoci s riešením a následným zdôvodnením a nápravou problémov a incidentov dostupnosti;
- Manažment kapacity: s poskytovaním pružnej a voľnej kapacity;
- Manažment kontinuity IT služieb: s odhadom obchodných vplyvov a rizík a poskytnutím odolnosti, po-chybových a obnovovacích mechanizmov;
- Manažment úrovní služieb: pomoc s určovaním cieľov dostupnosti a s preskúmavaním a riešením narušení služieb a komponent.

Proces riadenia dostupnosti v podstatnej miere závisí na meraní dosiahnutých výsledkov služieb a komponentov, ktoré sa týkajú dostupnosti. Platí, že: Ak to nemeriaš, nemôžeš to riadiť. Ak to nemeriaš, nemôžeš to zlepšiť. Ak to nemeriaš, pravdepodobne je ti to jedno. Ak to nemôžeš ovplyvniť alebo kontrolovať, tak to nemeraj.

Ako merať a podávať správy o dostupnosti IT služieb nevyhnutne závisí od toho, ktorá aktivita sa podporuje, kto sú príjemcovia a ako budú tieto informácie využité. Je podstatné rozpoznať odlišné perspektívy dostupnosti, aby meranie a podávanie správ uspokojovalo tieto rôznorodé potreby.

Za účelom uspokojenia rôznorodých perspektív dostupnosti musí riadenie dostupnosti zvážiť použitie celého radu meraní potrebných na informovanie o tej istej miere dostupnosti rozličnými spôsobmi. Merania musia mať zmysel a byť pridanou hodnotou, ak má byť celé meranie a podávanie správ o dostupnosti prínosom pre IT a obchodné organizácie.

[10] Operational Level Agreement, Dohoda o úrovni prevádzky.

2.2.4 Reaktívne aktivity manažmentu dostupnosti

1. Monitorovanie, meranie, analýza a vytváranie správ o dostupnosti služieb a komponentov

Kľúčovými výstupnými dátami z procesu riadenia dostupnosti je meranie a informovanie o dostupnosti IT služieb. Meranie dostupnosti by malo byť zapracované do SLA, OLA a ďalších podporných zmlúv. Na kontrolných stretnutiach pre úroveň služieb by tieto dohody mali byť pravidelne kontrolované a prehodnotené. Meranie a podávanie správ poskytuje základ pre:

- sledovanie skutočnej dostupnosti, ktorá bola poskytnutá, oproti dohodnutým cieľom;
- vytvorenie systému merania dostupnosti a dohodnúť s podnikom ciele týkajúce sa dostupnosti;
- určenie neprijateľných úrovní dostupnosti, ktoré majú dopad na podnik aj užívateľov;
- prekontrolovanie dostupnosti s IT podpornou organizáciou;
- neustále aktivity smerujúce k zlepšeniam za účelom optimalizácie dostupnosti.

Príkladmi tradičných meraní sú:

- **percento dostupnosti**: používa sa na porovnanie dosiahnutých výsledkov oproti dohodnutým cieľom v oblasti služieb;
- **percento nedostupnosti**: presný opak predošlého. Toto znázornenie má však výhodu, že sa zameriava na nedostupnosť. Má väčšiu šancu, že vytvorí povedomie o deficite v rámci poskytovania požadovanej úrovne dostupnosti;
- **trvanie**: dosiahne sa prepočítaním percent do hodín a minút;
- **frekvencia zlyhaní**: používa sa na zaznamenanie počtu prerušení IT služby;
- **dopad zlyhania**: je skutočné meradlo nedostupnosti služby.

Najdôležitejšími meradlami dostupnosti sú tie, ktoré odrážajú a merajú dostupnosť z podnikového a užívateľského hľadiska. Manažment dostupnosti musí zvažovať dostupnosť z oboch hľadísk, z hľadiska podniku (respektíve poskytovateľa IT služieb) a z hľadiska IT komponentov. Ide o úplne odlišné aspekty, a hoci je základná myšlienka totožná, meranie, hlavný predmet záujmu a dopady sú úplne odlišné.

Jediný dôvod pre všetky merania a správy, vrátane tých z podnikového hľadiska, je zlepšenie kvality a dostupnosti IT služieb pre podnik a užívateľov. Všetky merania, správy a aktivity by mali odzrkadľovať tento účel.

Dostupnosť, ktorú meriame a podávame o nej správy tak, aby odzrkadľovali skúsenosť užívateľov, vrátane tých z perspektívy podniku, poskytuje oveľa reprezentatívnejší pohľad na celkovú kvalitu IT služieb. Pohľad užívateľa na dostupnosť je ovplyvnený troma faktormi: frekvenciou prestojov, trvaním prestojov a rozsahom dopadu. Meranie a informovanie o dostupnosti z hľadiska užívateľa by preto malo tieto tri faktory zahŕňať.

2. Analýza nedostupnosti

Je nutné si uvedomiť, že nedostupnosť IT je spojená s nákladmi. Preto nedostupnosť IT tiež nie je zadarmo. Pre vysoko kritické podnikové systémy je nutné zvážiť nielen náklady poskytovania služieb, ale aj náklady vyplývajúce z ich zlyhania. Optimálnou rovnováhou je zvažovať náklady rôznych riešení dostupnosti oproti nákladom vyplývajúcim z nedostupnosti.

Náklady zlyhania IT by sa dali jednoducho vyjadriť ako počet podnikových či IT transakcií, ktoré boli ovplyvnené, buď ako reálne číslo, alebo založené na odhade. Ak sa výška nákladov meria oproti životne dôležitým funkciám (VBF), ktoré podporujú fungovanie podniku, je možné jednoznačne ukázať dôsledky zlyhania. Výhodou tohto prístupu je relatívna ľahkosť, s akou je možné získať informácie o účinkoch a žiadna potreba zložitých výpočtov. Tiež sa stáva hodnotou, ktorú takto chápe podnik aj IT organizácia. Tento prístup sa môže stať podnetom pre rozpoznávanie príležitostí na vylepšenie systému a môže sa stať kľúčovou veličinou pri sledovaní dostupnosti IT služieb.

Peňažná hodnota sa dá vypočítať kombináciou konkrétnych nákladov spojených so zlyhaním, ale tiež môže zahŕňať množstvo len ťažko definovateľných nákladov. Peňažná hodnota by mala odrážať dopad na celú organizáciu z nákladového hľadiska, t.j. podnik a IT organizácia. Konkrétne náklady môžu zahŕňať: strata užívateľskej produktivity, strata produktivity u zamestnancov IT, ušlý zisk, platby za nadčasy, vyplytvaný tovar a materiály, uvalené pokuty a tresty. Týmto nákladom dobre rozumie finančné oddelenie podniku a IT organizácie a je relatívne ľahšie vyjadriť a dať dohromady ich presnú výšku, než nekonkrétne náklady spojené so zlyhaním IT. Ťažko vyčísliteľné náklady môžu zahŕňať: nespokojnosť zákazníkov, strata zákazníkov, strata podnikateľských príležitostí, poškodenie dobrého mena podniku, strata dôvery v poskytovateľa IT služieb, poškodenie morálky zamestnancov. Nevyhýbajte sa ťažko vyčísliteľným nákladom len preto, že sú zle merateľné.

3. Rozšírený životný cyklus incidentov

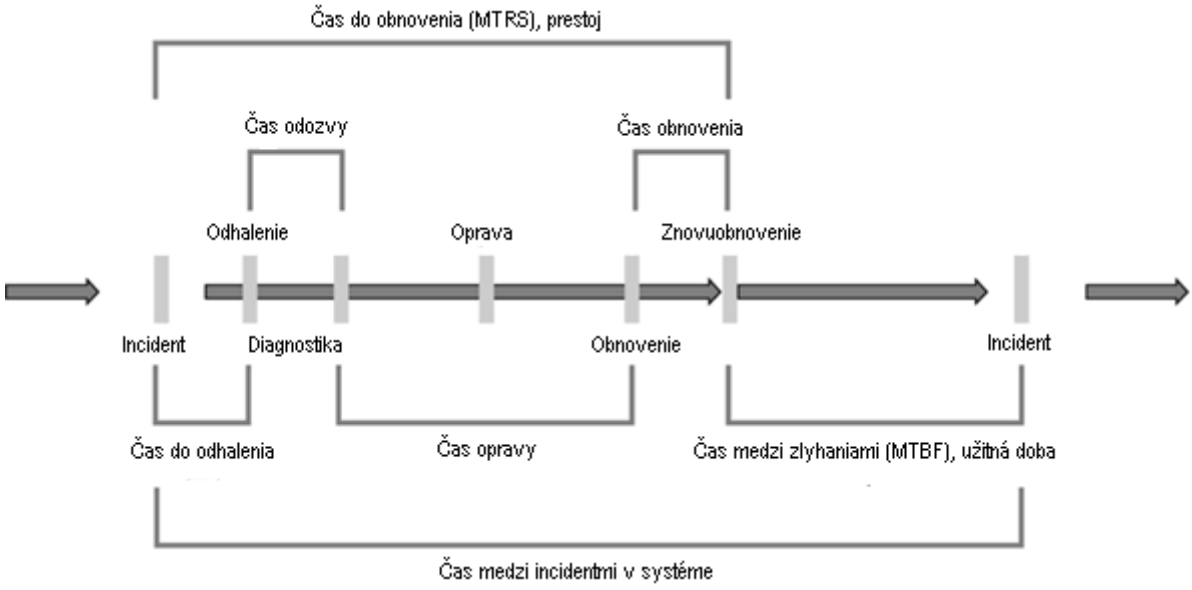
Cieľom riadenia dostupnosti je zaistiť, aby trvanie a dopady incidentov, ktoré majú vplyv na IT služby, boli minimálne, a aby bolo normálne fungovanie podniku obnovené čo najskôr.

Analýza rozšíreného životného cyklu incidentu umožňuje celkový prestoj IT služby rozobrať a zmapovať podľa hlavných fáz, ktorými incident prechádza.

Pohľad na udalosť z hľadiska jej životného cyklu je dobrá technika, ktorá napomáha technickej analýze toho, ako zlyhanie ovplyvnilo dostupnosť komponentov a služieb. Každý incident, udalosť prechádza viacerými fázami. Doba trvania jednotlivých fáz sa môže líšiť. Pre účely riadenia dostupnosti bol štandardný životný cyklus incidentov rozšírený za účelom poskytnutia dodatočnej pomoci a rád, najmä vo fáze návrhu na ozdravenie (viď obrázok 2.3). Pohľad na životný cyklus incidentu pomáha pri definovaní požiadaviek na odhaľovanie incidentov a nehôd, evidenciu diagnostických dát a nástrojov nutných na diagnostiku, plánovanie ozdravenia a overenie, či IT služba opäť funguje. Individuálne fázy životného cyklu sú nasledujúce:

- **Odhalenie incidentu** - čas, za ktorý poskytovateľ IT služby odhalí výskyt incidentu;
- **Diagnostika incidentu** - čas potrebný na určenie dôvodov zlyhania;
- **Oprava incidentu** - čas potrebný na opravu či vyriešenie incidentu, problému;
- **Obnovenie po incidente** - čas, za ktorý je možné dokončiť úplné ozdravenie po výskyte incidentu;
- **Znovuobnovenie, obnova po incidente -** čas potrebný na znovuobnovenie služby**.**

Každá fáza, a s ňou spojený čas, má vplyv na dĺžku trvania prestoju vnímanú zákazníkom. Tento prístup umožní odhaliť, kde presne bol tento čas stratený pri znovuobnovovaní služby. Tento prístup tiež umožní odhaliť neefektívne oblasti, kde straty pre podnik spojené s prestojom sú väčšie, než nevyhnutne musia byť.



Obr. 2.3 Rozšírený životný cyklus incidentov (zdroj [4], autorsky upravený)

4. Analýza zlyhania služby (SFA, Service Failure Analysis)

SFA je technika vytvorená pre štrukturálny prístup na identifikáciu zásadných príčin opakujúcich sa prerušení služby u užívateľa, využíva celý rad zdrojových dát na určenie a zhodnotenie, prečo sa tieto nedostatky v nedostupnosti vyskytujú. SFA sa riadi ako úloha alebo projekt a využíva aj iné techniky a metódy riadenia dostupnosti smerujúce k formulácii návrhov na zlepšenie. Detailná analýza príčin zlyhania služby môže odhaliť potenciálny priestor pre zvýšenie dostupnosti. SFA je štruktúrovaná technika na odhalenie návrhov na vylepšenie celkovej dostupnosti, ktorá prinesie výhody pre užívateľov. Mnoho týchto aktivít v rámci SFA je spojených s riadením problémov a v mnohých organizáciách sú tieto aktivity vykonávané spoločne riadením dostupnosti a riadením problémov.

Cieľom SFA je zlepšenie celkovej dostupnosti IT služieb: prípravou návrhov na vylepšenie pre okamžitú implementáciu alebo pre plán dostupnosti, identifikáciou zásadných príčin výskytu zlyhania IT služieb u užívateľov, zhodnotením efektivity IT podpornej organizácie a kľúčových procesov, vytvorením správ opisujúcich najdôležitejšie závery a odporúčania. Vylepšenia vyplývajúce z aktivít SFA by mali byť merané.

Kvôli maximalizácii času pre jednotlivcov pracujúcich na úlohách SFA a zvýšeniu kvality výsledných správ sa vyžaduje štruktúrovaný prístup. Tento prístup je podobný poradenským modelom využívaným v rámci odvetvia a istým spôsobom poskytuje podniku interné poradenstvo.

Štruktúra SFA:

- **Výber príležitosti** - pred zadaním úlohy SFA sa musí dohodnúť, ktorá IT služba či technológia sa vyberie;
- **Rozsah úlohy -** presné určenie, ktoré oblasti sú a nie sú súčasťou úloh, v písomnej forme ešte pred zadaním úlohy;
- **Plánovanie úlohy** - aktivity v rámci SFA musia byť naplánované a odsúhlasené celé týždne pred začatím úlohy s dohodnutým plánom projektu a presne určenými zdrojmi;
- **Vytvorenie hypotézy -** užitočná metóda vytvorenia pravdepodobných scenárov, ktoré umožnia dospieť k rýchlym záverom ešte počas analytickej fázy;
- **Analýza dát** - v rámci tímu sa rozdelia role a zodpovednosť v rámci analyzovania dát. Počas analytickej fázy zoznam hypotéz pomáha načrtnúť niektoré predčasné závery;

- **Rozhovory s kľúčovými zamestnancami** - tento dialóg môže priniesť veľmi rýchle príležitosti, a jednoduché IT riešenie vyrieši to, čo vnímal podnik ako veľký problém, preto sa s týmito rozhovormi začne čo najskôr po začatí projektu;
- **Zistenia a závery** - po analýze zhromaždených dát, rozhovoroch a neustálej revízii zoznamu hypotéz by mal byť tím pripravený na zdokumentovanie prvotných zistení a záverov. Je tiež dôležité podniknúť dodatočné analýzy na overenie zistení, tak aby všetky zistenia a závery boli jasne podložené zozbieranými dôkazmi;
- **Odporúčania** - po overení všetkých záverov a zistení by mal byť tím pripravený na formuláciu odporúčaní. Cieľom je identifikácie doporučení, ktoré sú praktické a po implementácii udržateľné;
- **Správa** - záverečná správa by mala byť vyhotovená pre sponzora spolu so súhrnom pre manažment. Štýl správy si určí každá organizácia sama;
- **Overenie** - kvôli investovanému času a úsiliu na dokončenie SFA je nutné po zverejnení odporúčaní a súhlase sponzora prikročiť k ich implementácii. Úspech celého projektu SFA je nutné po celý čas sledovať a merať kvôli neustálej efektivite.

2.2.5 Pro-aktívne aktivity manažmentu dostupnosti

Schopnosti procesu manažment dostupnosti sú pozitívne ovplyvnené počtom a kvalitou využívaných pro-aktívnych metód a techník.

1. Identifikácia životne dôležitých funkcií podniku (VBF, Vital Business Function)

Pojem životne dôležitá funkcia podniku (VBF) sa používa na opis tých životne dôležitých elementov podnikových procesov, ktoré sú podporované IT službami. Služby tiež môžu podporovať menej dôležité podnikové funkcie, ale VBF je dôležité zdokumentovať preto, aby bolo možné zaručiť úplné stotožnenie sa s biznisom.

2. Návrh pre dostupnosť

Podnikom vyžadovaná úroveň dostupnosti má vplyv na celkovú úroveň nákladov poskytovaných IT služieb. Vo všeobecnosti platí, čím vyššia úroveň dostupnosti, tým vyššie náklady. Nejedná sa len o náklady spojené so sprostredkovaním základných IT technológií a vyžadovaných služieb podporujúcich IT infraštruktúru. Dodatočné náklady sú spojené s poskytovaním vhodných procesov riadenia služieb, systematických manažérskych nástrojov a riešení zabezpečujúcich vysokú dostupnosť nutných na splnenie prísnejších požiadaviek na dostupnosť. Pri úvahách o spôsobe, akým naplniť požiadavky podniku na dostupnosť,

je dôležité zabezpečiť, aby úroveň dostupnosti, ktorá má byť poskytnutá IT službami, bola na úrovni, ktorá sa očakáva, podnik si ju mohol dovoliť a podnik vnímal výšku nákladov ako oprávnenú. Obrázok 2.4 ukazuje produkty a procesy potrebné pre poskytovanie rôznych úrovní dostupnosti a nákladové dôsledky. Tieto produkty a procesy sú:

Základné produkty a komponenty. Zadováženie či vývoj základných produktov, technológií a komponentov by malo byť závislé na ich schopnosti splniť najprísnejšie požiadavky na dostupnosť a spoľahlivosť. To by malo byť základom celého návrhu dostupnosti. Dodatočné investície vyžadované na dosiahnutie vyššej úrovne dostupnosti vyjdú nazmar a daná úroveň dostupnosti nebude dosiahnutá v prípade, že základné produkty a komponenty sú nespoľahlivé a majú sklony k poruchám.

Manažment systémov, by mal poskytnúť monitorovanie, diagnostiku a automatickú nápravu chýb na rýchle odhalenie a vyriešenie potenciálnych a aktuálnych problémov a zlyhaní.

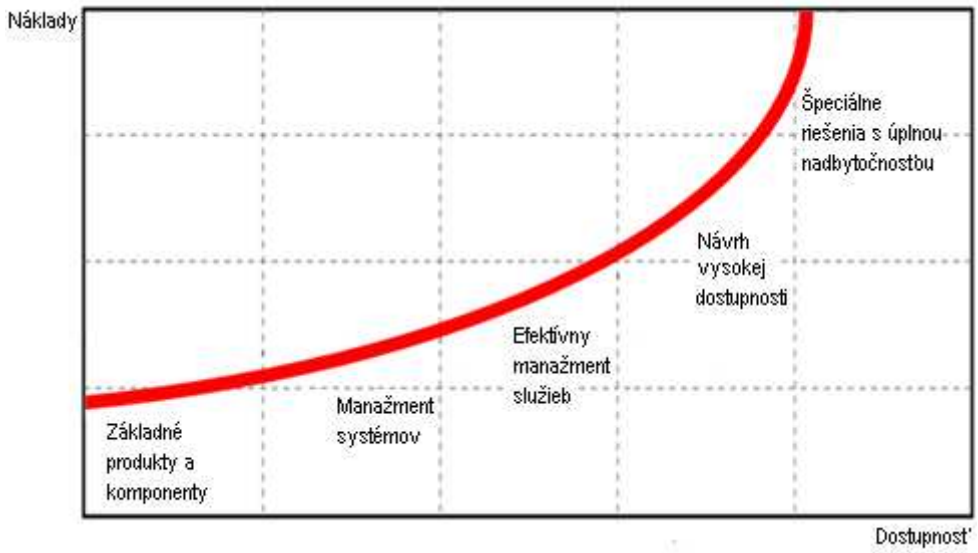
Procesy riadenia služieb. Efektívne procesy riadenia dostupnosti prispievajú k vyšším úrovniam dostupnosti. Procesy ako riadenie dostupnosti, problémov a incidentov, riadenie zmien a konfiguračný manažment hrajú kľúčovú rolu pri riadení celkových IT služieb.

Návrh vysokej dostupnosti, musí zvážiť odstránenie SPoF alebo poskytnutie alternatívnych komponentov tak, aby narušenie podnikových operácií bolo minimálne v prípade výskytu zlyhania. Návrh musí tiež zohľadniť zníženie či minimalizáciu efektov plánovaných prestojov na normálne fungovanie podniku nutných na poskytnutie údržby, implementáciu zmien IT infraštruktúry alebo obchodných aplikácií. Kritériá na ozdravenie by mali definovať rýchle ozdravenie a znovuobnovenie IT služieb ako kľúčový cieľ v rámci fáze návrhu na ozdravenie.

Špeciálne riešenia s úplnou nadbytočnosťou, prístup neustálej dostupnosti so 100% rozsahom vyžaduje nákladné riešenia s úplným zrkadlením alebo nadbytočnosťou. Nadbytočnosť je metóda na zlepšovanie dostupnosti využívajúca duplicitné komponenty. Na splnenie prísnych požiadaviek na dostupnosť musia tieto riešenia pracovať autonómne v paralele. Tieto riešenia sa neobmedzujú len na IT komponenty, ale tiež na IT prostredia, ako dátové centrá, dodávky energií a telekomunikácie.

Dôležitosť, ktorá sa pripisuje skorej účasti pri návrhu IT infraštruktúry, by sa nemala podceniť. Musí existovať dialóg medzi podnikom a IT na určenie rovnováhy medzi podnikovým vnímaním nákladov nedostupnosti a vysokých nákladov na poskytnutie vyššej úrovne dostupnosti.

Ako vidieť na obrázku 2.4, existuje významný nárast nákladov tam, kde podnikové požiadavky na optimálnu úroveň dostupnosti sú vyššie než existujúca IT infraštruktúra dokáže doručiť. Tieto zvýšené náklady sú spôsobené významnými zmenami v návrhu technológie a meniacimi sa požiadavkami na IT podpornú organizáciu.



Obr. 2.4 Vzťah medzi úrovňou dostupnosti a celkovými nákladmi (zdroj [4], autorsky upravený)

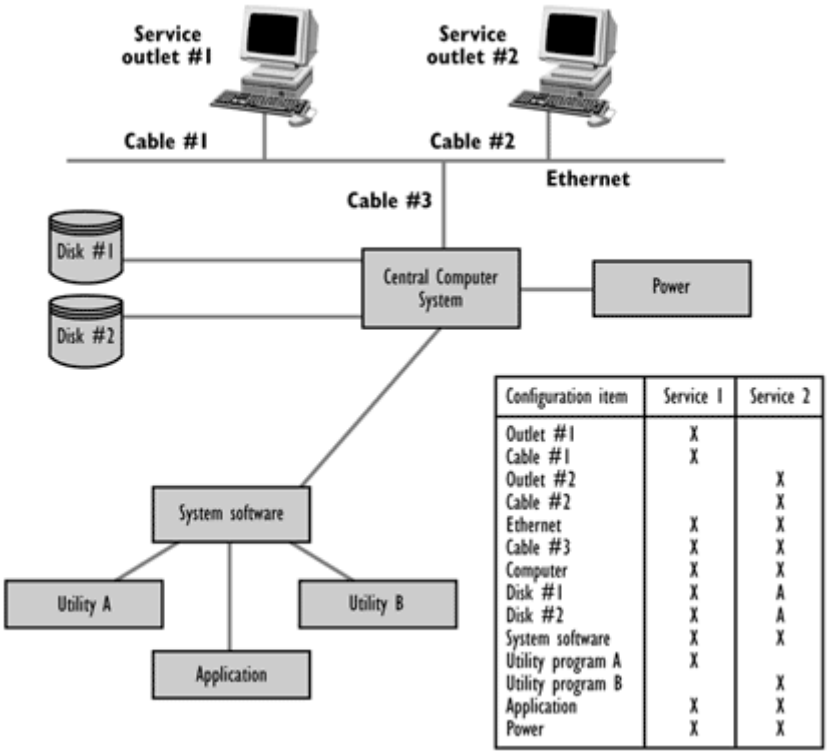
3. Analýza dopadu zlyhania komponentu (CFIA, Component Failure Impact Analysis)

CFIA sa používa na predpovedanie a hodnotenie dopadov na IT službu v dôsledku zlyhania v rámci technológie. Výstupné dáta z CFIA môžu byť použité na identifikáciu možného zváženia dodatočnej odolnosti na zníženie či minimalizáciu dopadu zlyhania IT služby na fungovanie podniku a užívateľov. To je obzvlášť dôležité vo fáze návrhu služby, kde je nutné odhadnúť a zhodnotiť dopad na dostupnosť IT služby vyplývajúci zo zlyhania IT komponentov v rámci návrhu IT služby. Metódu je tiež možné aplikovať už na existujúce služby a infraštruktúru.

Výstupom CFIA sú dôležité informácie, ktoré ovplyvnia návrhové kritériá na dostupnosť a ozdravenie tak, aby podnikové operácie a užívatelia boli ovplyvnení v minimálnej miere v prípade zlyhania IT služby. CFIA toto dosiahne poskytnutím a naznačením:

- SpoF, ktoré majú vplyv na dostupnosť;
- Dopadom zlyhania IT služby na podnikové funkcie a užívateľov;
- Závislostí medzi ľuďmi a komponentmi;
- Časov potrebných na ozdravenie komponentov;
- Potreby identifikovať a zdokumentovať možnosti ozdravenia;
- Potreby identifikovať a implementovať opatrenia na zníženie rizika.

Na hodnotenie určenej konfigurácie IT infraštruktúry je prvým krokom vytvorenie súradnicovej siete s CI na jednej osi a IT službami, ktoré sú závislé na CI, na druhej osi, tak ako je to znázornené na obrázku 2.5.



Configuration item	Service 1	Service 2
Outlet #1	X	
Cable #1	X	
Outlet #2		X
Cable #2		X
Ethernet	X	X
Cable #3	X	X
Computer	X	X
Disk #1	X	A
Disk #2	X	A
System software	X	X
Utility program A	X	
Utility program B		X
Application	X	X
Power	X	X

Obr. 2.5 Analýza dopadu zlyhania komponentu (CFIA) (zdroj [4])

Vyplnenie súradnicovej siete:

- Prázdne pole, ak zlyhanie CI žiadnym spôsobom neovplyvní službu;
- X, ak zlyhanie CI spôsobí, že služba je nefunkčná;
- A, ak existuje alternatívna CI, ktorá službu vykoná;
- M, ak existuje alternatívne CI, ktoré službu vykoná, ale je potrebný manuálny zásah na obnovenie služby.

Pre detailnejšiu analýzu je nutné rozšíriť CFIA maticu o ďalšie polia, ako napríklad: pravdepodobnosť zlyhania, časový odhad obnovenia CI, obnovovacie procedúry, vzťahy závislosti medzi CI a iné.

4. Analýza jednotného zdroja zlyhania (SPoFA, Single Point of Failure Analysis)

SPoF je taký komponent v IT infraštruktúre, ktorý nemá implementované protiopatrenia a má potenciál zapríčiniť prerušenie biznisu, zákazníka alebo užívateľa, keď zlyhá. Je dôležité, aby neexistoval žiadny nerozpoznaný SPoF v návrhu IT infraštruktúry a ani v terajšej technológii, a aby sa im predchádzalo všade, kde to ide. Použitie SPoF analýzy

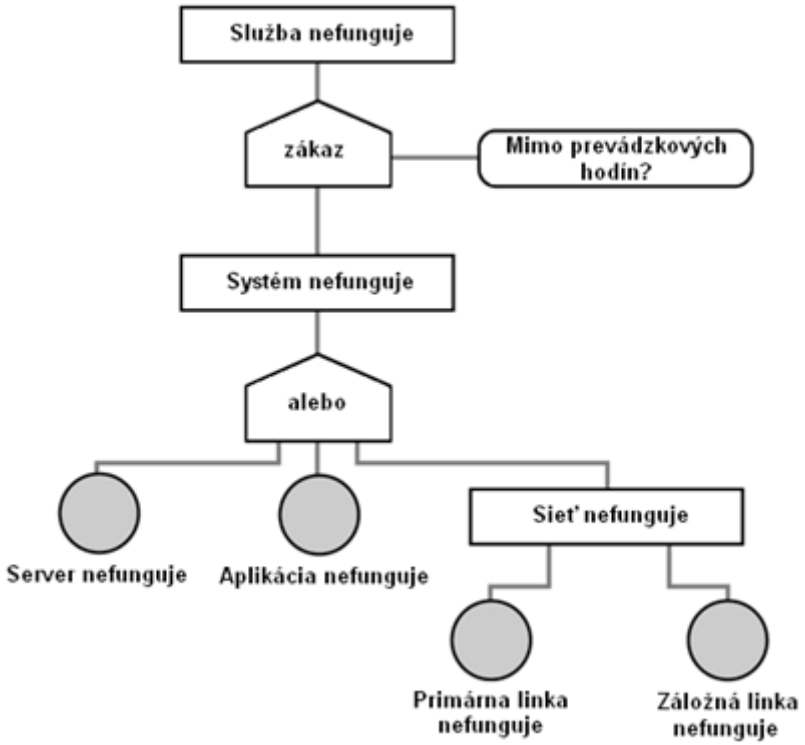
alebo CFIA ako metódy na identifikáciu SPoF sa odporúča. Uplatňovanie SPoF a CFIA analýz by malo byť vykonávané pravidelne, a kdekoľvek je SPoF nájdený, CFIA môže byť použitá na identifikáciu potenciálnych obchodných, zákazníckych a užívateľských vplyvov a pomáha určiť, ktoré alternatívy môžu alebo by mali byť uvážené pri zohľadnení tejto slabosti v návrhu alebo v terajšej technológii.

5. Analýza stromu chýb (FTA, Fault Tree Analysis)

FTA je metóda, ktorá môže byť použitá na určenie reťaze udalostí, ktorá spôsobila narušenie IT služieb. FTA, v spojení s výpočtovými metódami, môže ponúknuť detailné modely dostupnosti. Môže byť použitá na hodnotenie zlepšenia dostupnosti, ktoré môže byť dosiahnuté možnosťami návrhu jednotlivých technologických komponentov. Použitie FTA:

- môže poskytnúť informácie, ktoré môžu byť použité pre výpočty dostupnosti;
- môžu byť vykonané operácie na výslednom strome chýb, tieto operácie korešpondujú s možnosťami návrhu;
- môže byť v analýzach zvolená požadovaná úroveň podrobnosti.

FTA znázorňuje reťazec udalostí použitím Boolean zápisu. Na obrázku 2.6 môžete vidieť príklad stromu chýb.



Obr. 2.6 Príklad analýzy stromu chýb (FTA) (zdroj [4], autorsky upravený)

FTA rozoznáva nasledujúce udalosti:

- **Základné udalosti** - koncové body stromu chýb, už sa nedajú rozložiť do väčšej hĺbky, ak áno, jedná sa o vyplývajúce udalosti;
- **Vyplývajúce udalosti** - prechodné uzly, vyplývajúce z kombinácie udalostí;
- **Podmienené udalosti** - udalosti, ktoré nastanú len za určitých podmienok;
- **Spúšťacie udalosti** - udalosti, ktoré spúšťajú ďalšie udalosti.

Tieto udalosti sú spájané pomocou logických operátorov, ako napríklad:

- **A** - vyplývajúca udalosť nastane, len keď všetky vstupné udalosti nastanú súčasne;
- **Alebo** - vyplývajúca udalosť nastane, keď nastane jedna alebo viac vstupných udalostí;
- **Výlučné alebo** - vyplývajúca udalosť nastane, keď nastane jedna a len jedna z vstupných udalostí;
- **Zákaz** - vyplývajúca udalosť nastane len, keď vstupná podmienka nie je splnená.

6. Modelovanie

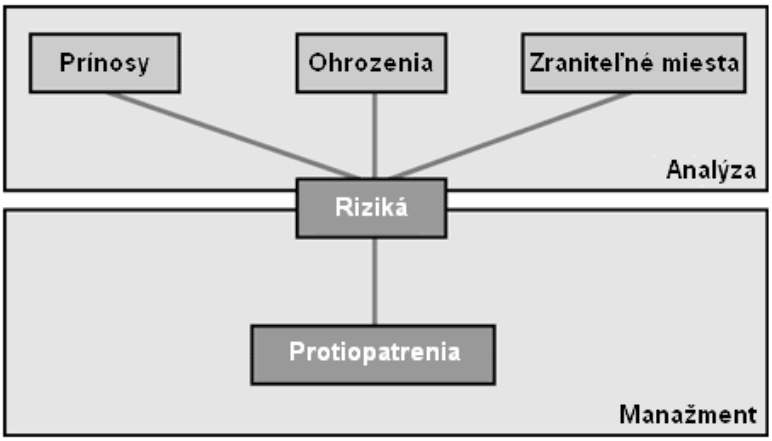
Odhadnúť v rámci návrhu, či nové komponenty môžu dosiahnuť stanovené požiadavky, je dôležité na to, aby testovací režim zaručil, že požadovaná dostupnosť môže byť doručená. Nástroje na simulácie a modelovanie by mali pri vytvorení očakávaného užívateľského dopytu po nových službách seriózne posúdiť, či komponenty pokračujú v prevádzke v očakávaných objemových a stresových podmienkach. Nástroje na modelovanie slúžia tiež na predpovedanie dostupnosti a na hodnotenie dopadov zmien na IT infraštruktúru.

7. Riadenie a analýza rizík

Riadenie a analýza rizík je metóda, ktorá sa používa na identifikáciu a ohodnotenie rizík a oprávnené protiopatrenia, ktoré môžu byť implementované na ochranu dostupnosti IT systémov. Identifikácia rizík a poskytovanie oprávnených protiopatrení na redukciu a elimináciu hrozieb predstavovaných týmito rizikami môže hrať dôležitú úlohu v dosahovaní vyžadovaných úrovní dostupnosti nových alebo vylepšených IT služieb. Analýza rizík by mala byť urobená počas fázy návrhu IT technológie a služby na identifikáciu:

- Rizík, ktoré môžu spôsobiť nedostupnosť IT komponentov v technológii a v návrhu služieb;
- Rizík, ktoré môžu spôsobiť odhalenia dôvernosti a integrity v technológii a v návrhu služieb.

Väčšina metodológií riadenia a posúdenia rizík si vyžaduje použitie formálneho prístupu k posúdeniu rizík a následnému znižovaniu rizika zavedením nákladovo oprávnených protiopatrení, ako je to vidieť na obrázku 2.7.



Obr. 2.7 Analýza a manažment rizík (zdroj [4], autorsky upravený)

Keď aplikujete tento prístup pomocou formálnej metódy, musíte zaistiť, aby:

- všetky možné riziká a protiopatrenia boli identifikované;
- všetky zraniteľné miesta boli identifikované a ich úrovne presne stanovené;
- všetky hrozby boli identifikované ich úrovne presne stanovené;
- všetky výsledky sú dôsledne revidované;
- všetky výdavky na zvolené protiopatrenia sú oprávnené.

Formálne metódy analýzy a riadenia rizík sú teraz dôležitým elementom v celkovom návrhu a poskytovaní IT služieb. Posúdenie rizika je často založené na pravdepodobnosti a možných dopadoch jeho výskytu. Protiopatrenia sú zavedené tam, kde sú nákladovo oprávnené pri redukcii dopadov udalostí alebo pravdepodobnosti, že sa udalosť stane, alebo pri redukcii oboch.

8. Plán testovania dostupnosti

Plán testovania dostupnosti je plán pre pravidelné testovanie všetkých mechanizmov dostupnosti. Niektoré mechanizmy dostupnosti, ako vyvažovanie načítania, sa používajú denne, iné sa používajú len po zlyhaniach. Preto je podstatné, aby všetky mechanizmy dostupnosti boli testované pravidelným a plánovaným spôsobom na zaistenie toho, že ak budú naozaj potrebné, budú fungovať.

9. Plánovaná a preventívna údržba

Všetky IT komponenty by mali byť subjektom pre stratégiu plánovanej údržby. Frekvencia a úroveň vyžadovanej údržby sa líši komponent od komponentu. Plánovaná údržba umožňuje IT podpornej organizácii zaistiť:

- Preventívnu údržbu, aby sa predišlo zlyhaniam;
- Plánovať SW a HW upgrady na zaistenie novej funkcionality alebo pridania kapacity;
- Podnikom požadované zmeny v podnikových aplikáciách;
- Implementáciu nových technológií a funkcionalít pre podnikové účely.

Najvhodnejší čas na zaradenie plánovaného prestoja je vtedy, keď sú jeho dopady na podnik a jeho zákazníkov najmenšie. Pri určovaní požiadaviek na dostupnosť pre nové alebo vylepšené IT služby by malo byť množstvo prestojov a z toho vplývajúca strata príjmov kvôli plánovanej odstávke pre podnik neakceptovateľné. Hlavne pri 24 x 7 prevádzke služieb musí byť údržba vykonaná bez vplyvu na dostupnosť IT služieb.

10. Vytvorenie dokumentu Projected Service Outage[11] (PSO)

Manažment dostupnosti by mal vytvoriť a udržiavať dokument PSO. Tento dokument pozostáva z odchýlok od dostupnosti služby dohodnutej v SLA. Môže byť vytvorený na základe vstupov z: plánov zmien, plánov releasov, plánu plánovaných a preventívnych údržieb, plánov testovania dostupnosti, plánov ITSCM a BCM testovania. PSO obsahuje detaily všetkých plánovaných prestojov služieb v rámci dohodnutých hodín prevádzky služieb pre všetky služby. Tieto dokumenty by mali byť schválené všetkými príslušnými oddeleniami a zástupcami podniku i IT.

11. Neustála revízia a zlepšovanie

Zmena obchodných potrieb a užívateľských požiadaviek si môže vyžiadať, aby boli úrovne poskytovanej dostupnosti IT služieb revidované. Dôležitosť služieb sa bude často meniť a je dôležité, aby návrh a technologická podpora takýchto služieb bola pravidelne revidovaná a zdokonaľovaná manažmentom dostupnosti, aby bolo zaistené, že zmena dôležitosti služby sa odráža v revidovanom návrhu a podpornej technológii.

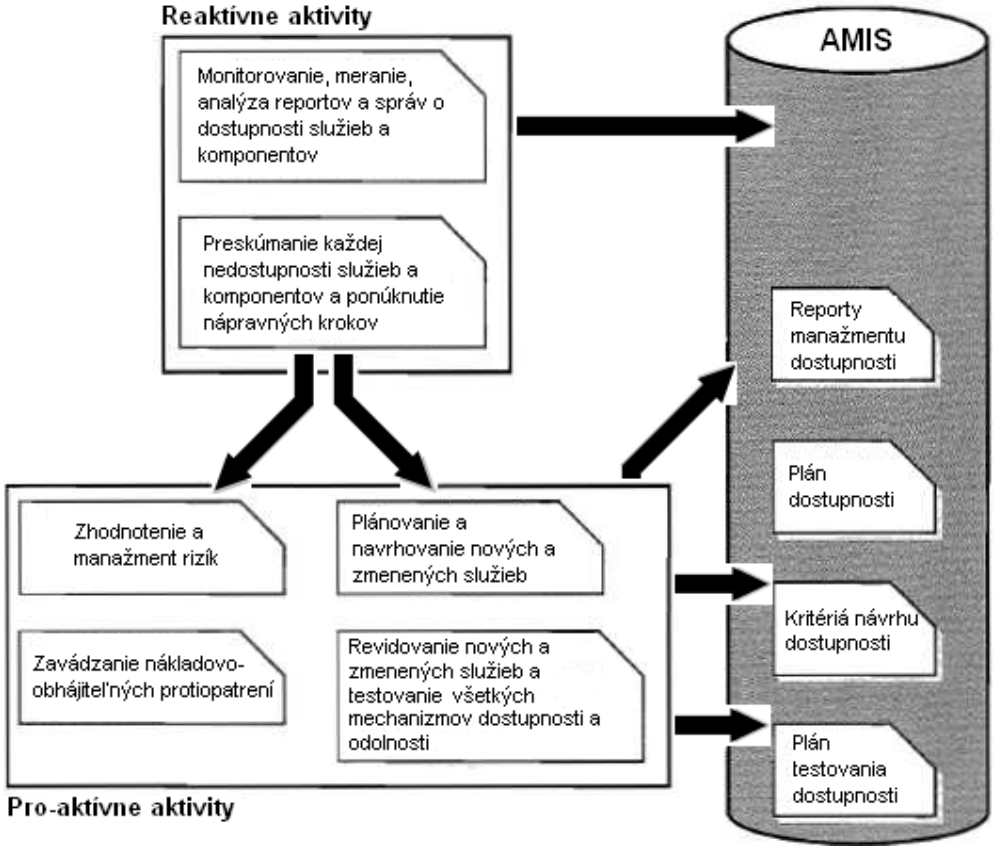
Kľúčová činnosť manažmentu dostupnosti je neustále hľadať možnosti optimalizácie dostupnosti IT infraštruktúry v spojení s aktivitami neustáleho zlepšovania služieb. Prínosy

[11] Plánovaný výpadok služby. Dokument, ktorý identifikuje efekt plánovaných zmien, údržbových aktivít a plánov testovania na dohodnutých úrovniach služieb. [13]

tohto prístupu sú, že niekedy môžu byť dosiahnuté vyššie úrovne dostupnosti, ale s omnoho nižšími nákladmi. Je možno aplikovať množstvo techník na identifikáciu príležitostí na optimalizáciu. Odporúča sa nezameriavať sa len na technológiu, ale tiež na revidovanie podnikových procesov a iných komplexných obchodných úloh. Na dosiahnutie týchto cieľov potrebuje byť manažment dostupnosti rozpoznaný ako rozhodujúci vplyv v organizácii poskytovateľa IT služieb na zaistenie neustáleho zamerania sa na dostupnosť a stabilitu technológie.

2.2.6 Availability Management Information System[12]

Proces manažment dostupnosti by mal udržiavať Availability Management Information System (AMIS), ktorý obsahuje všetky merania a informácie potrebné na doplnenie procesu manažment dostupnosti a ktorý poskytuje podniku informácie o úrovni poskytovaných IT služieb. Tieto informácie, týkajúce sa služieb, komponentov a podporných služieb, poskytujú základ pre pravidelné, ad hoc a výnimočné správy o dostupnosti a identifikuje trendy v rámci údajov na stimuláciu zlepšovacích aktivít. Tieto aktivity a informácie obsiahnuté v AMIS poskytujú základ pre rozvíjanie obsahu plánu dostupnosti.



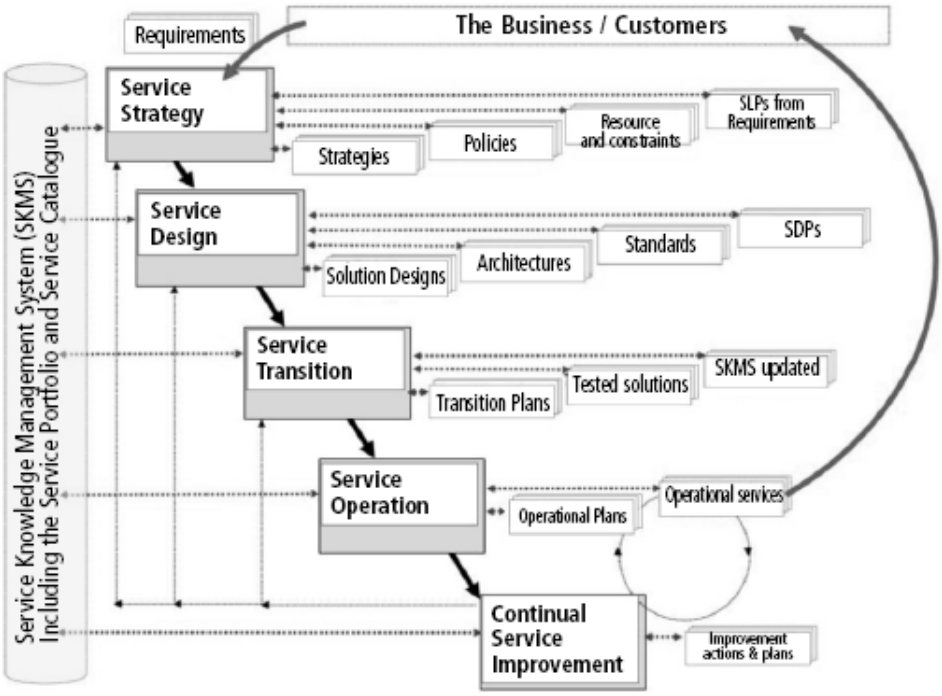
Obr. 2.8 Proces manažment dostupnosti a AMIS (zdroj [4], autorsky upravený)

[12] Informačný systém pre manažment dostupnosti.

3 Analýza užívateľských potrieb v oblasti dostupnosti IT služieb v malých a stredných firmách

3.1 ITIL odporúčania pre užívateľské požiadavky

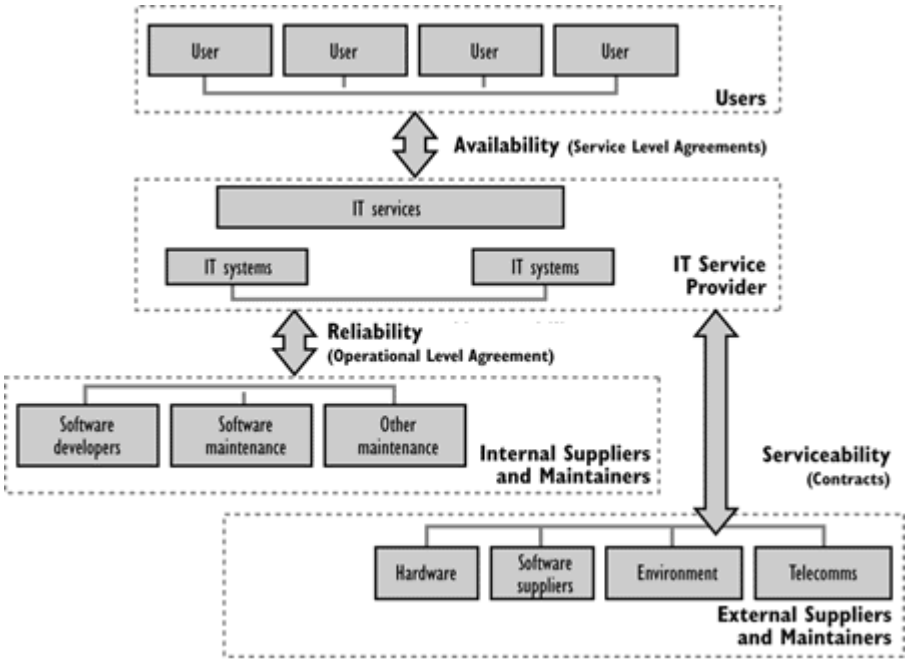
Všetky riešenia a aktivity služieb by mali byť riadené obchodnými potrebami a požiadavkami, a preto sa tieto požiadavky musia tiež odrážať v stratégii a politike organizácie, ktorá poskytuje IT služby, ako je to na obrázku 3.1. Z obrázku je zrejmé, že životný cyklus služby začína zmenou v požiadavkách podniku alebo zákazníka. Tieto požiadavky sú stanovené a dohodnuté vo fáze stratégia služieb v rámci Service Level Package (SLP). [3]



Obr. 3.1 Kľúčové odkazy, vstupy a výstupy etáp životného cyklu služby (zdroj [3])

Existuje mnoho spôsobov, ako môžete definovať požiadavky na dostupnosť. ITIL odporúčajú použiť dohody o úrovni služby (SLA) na definovanie požadovaných hodín prevádzky kľúčových služieb. Manažment úrovní služieb (SLM [13]) je zodpovedný za komunikáciu s podnikom o tom, ako budú podnikové požiadavky na dostupnosť splnené a za vyjednávanie o obsahu a uzatváranie SLA, dohôd o úrovni prevádzky (OLA) a podporných kontraktov (UC) a ich následné vyhodnocovanie (viď obrázok 3.3). Riadenie dostupnosti preto poskytuje dôležitú podporu a vstup pre SLM. [5], [16]

[13] Cieľom procesu SLM je udržovať a zlepšovať kvalitu IT služieb a vytvárať pozitívny vzťah medzi úsekom ICT a jeho zákazníkmi.



Obr. 3.2 Vzťahy s dodávateľmi a údržbármi IT infraštruktúry (zdroj [4])

ITIL odporúča, aby podnikové požiadavky na dostupnosť IT služieb minimálne obsahovali: definíciu kriticky dôležitých podnikových funkcií podporovaných IT službou, definíciu prestojov IT služby (podmienky, za ktorých sa považuje IT služba za nedostupnú), dopady na podnik spojené so stratou služby a s tým spojenými rizikami, kvantitatívne požiadavky na dostupnosť (do akej miery podnik toleruje prestoje či zhoršenú kvalitu IT služieb), vyžadovaný počet servisných hodín (kedy má byť služba poskytovaná), hodnotenie relatívnej dôležitosti rozličnej pracovnej doby, špecifické požiadavky na bezpečnosť, servisná podpora a schopnosti obnovenia.[5]

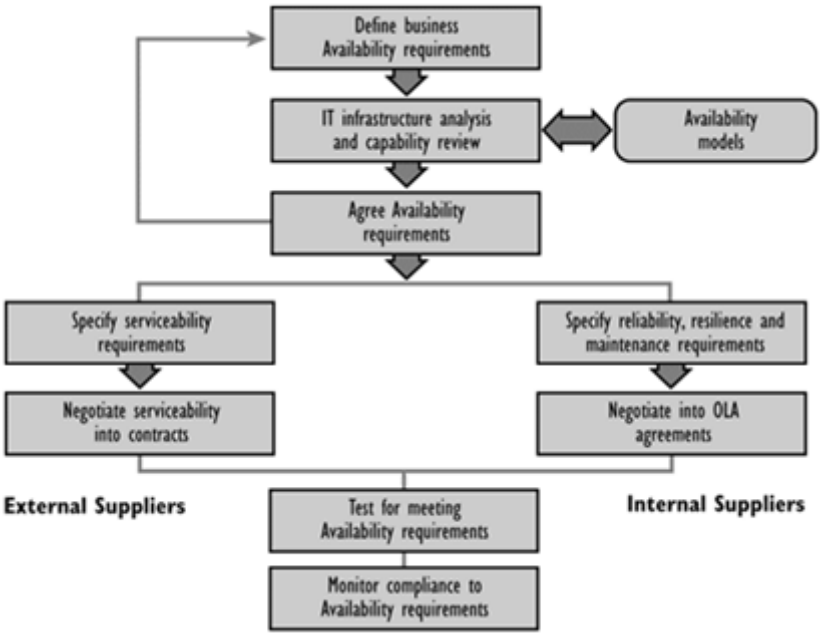
Akonáhle sú požiadavky na IT technológiu a IT podpornú organizáciu hotové, poskytovateľ IT služieb je v pozícii, kedy má potvrdiť, či je možné požiadavky na dostupnosť splniť. Tam, kde sa odhalia nedostatky, je nutné diskutovať s podnikom o nákladových možnostiach na rozšírenie poskytnutého návrhu schopných splniť vyžadovanú úroveň dostupnosti. Podnik má možnosť prehodnotiť, či potrebuje vyššie alebo nižšie úrovne dostupnosti a tiež porozumieť dôsledkom svojich rozhodnutí a nákladom s nimi spojenými. [5]

Určenie požiadaviek na dostupnosť je opakovaným procesom, obzvlášť tam, kde je nutné dať do rovnováhy podnikové požiadavky na dostupnosť oproti relevantným nákladom. Potrebnými krokmi sú (pre názornosť viď obrázok 3.3):

- určiť dopady na podnik vyplývajúce zo straty služby;

- z podnikových požiadaviek je nutné špecifikovať požiadavky v oblasti dostupnosti, spoľahlivosti a udržateľnosti pre IT služby a komponenty podporované IT podpornou organizáciou;
- pre externe dodávané služby a komponenty je nutné určiť požiadavky na servisovateľnosť;
- odhadnúť náklady spojené s požiadavkami na dostupnosť, spoľahlivosť, udržateľnosť a servisovateľnosť;
- spolu s podnikom určiť, či náklady na splnenie požiadaviek na dostupnosť sú odôvodnené;
- určenie výšky nákladov spojených so stratou či znížením kvality služieb;
- tam, kde je výška nákladov pre podnik prijateľná, požiadavky na dostupnosť, spoľahlivosť a udržateľnosť sú dohodnuté a ďalej sú predmetom rokovaní s cieľom uzavrieť zmluvy. [5]

Pre lepšie pochopenie niektoré tieto kroky popíšem v návrhovej časti na príklade.



Obr. 3.3 Vývoj požiadaviek na dostupnosť IT služieb (zdroj [4])

Tam, kde je výška nákladov neprijateľná, môžete buď:

- prehodnotiť návrh IT infraštruktúry, poskytnúť alternatívy s nižšími nákladmi a zhodnotiť dôsledky pre dostupnosť;
- prehodnotiť použitie a spoliehanie sa podniku na IT služby a prerokovať ciele dostupnosti v rámci SLA. [5]

3.2 Požiadavky na dostupnosť IT služieb

Túto časť som vypracoval pomocou materiálov, ktoré sú v použitej literatúre uvedené pod označením [12]. Predtým, ako budete môcť určiť požiadavky na dostupnosť, musíte zistiť, čo užívatelia naozaj potrebujú a očakávajú. Tieto názory pomáhajú určiť najlepšiu definíciu dostupnosti pre danú organizáciu.

Z hľadiska zákazníka sa hodnota skladá z dvoch základných prvkov: užitočnosť alebo vhodnosť na daný účel a záruka alebo vhodnosť použitia. [14]

- **Užitočnosť** - vníma zákazník z atribútov služby, ktoré majú pozitívny vplyv na plnenie úloh v spojení s požadovanými výsledkami. Odstránenie alebo zmiernenie obmedzení výkonu je tiež vnímané ako pozitívny účinok;
- **Záruka** - je odvodená z pozitívneho vplyvu, ktorý je v prípade potreby dostupný v dostatočnej miere alebo veľkosti, a spoľahlivý, pokiaľ ide o kontinuitu a bezpečnosť.

Príliš veľa IT organizácií sa zameriava na poskytovanie vysokej dostupnosti na základe definície IT oddelenia. V praxi však je koncový užívateľ ten, kto určuje, či je systém skutočne dostupný. V nasledujúcom texte ponúkam priame návrhy stanovenia definícií a požiadaviek na realistickú dostupnosť, ktoré môžu pomôcť pri predchádzaní niektorých dôsledkov neprijateľných úrovní dostupnosti.

Prvým krokom pri plánovaní dostupnosti je zistiť skutočné užívateľské požiadavky na dostupnosť a na IT služby vo všeobecnosti. To si vyžaduje konzultácie s čo najväčším možným počtom užívateľov alebo aspoň so všetkými užívateľmi kritických aplikácií. Prvá reakcia väčšiny užívateľov je, že systém musí byť k dispozícii stále. Je nutné objasniť, že náklady na poskytovanie dostupnosti systému sa s nárastom vyžadovanej dostupnosti neúmerne zvyšujú. Tiež je nutné vysvetliť, že tieto náklady budú nejakým spôsobom prenesené na užívateľov, či už priamo, alebo nepriamo.

3.2.1 Dohoda o úrovní služieb (SLA)

Existuje mnoho spôsobov, ako môžete definovať požiadavky na dostupnosť. ITIL odporúčajú použiť dohody o úrovni služby (SLA) na definovanie požadovaných hodín prevádzky kľúčových služieb. [16]

Konzultácie s užívateľmi tvoria základ pre dohodu o úrovni služieb (SLA) medzi poskytovateľom IT služieb a užívateľov. SLA môže byť obmedzená na jednoduchú dohodu, ktorá pokrýva práve dostupnosť systému, ale môže byť tiež rozšírená, aby zahŕňala čas

odozvy, dostupnosť help desku, čas obrátky požiadavky na novú funkciu a mnoho ďalších výkonnostných a kvalitatívnych otázok. Ak začínate od nuly, odporúčam zahrnúť len časť dostupnosti systému. Neskôr, keď sa systém stabilizuje a vaša IT organizácia bude vyspelejšia, môže byť SLA rozšírená. Tento prístup má mnoho výhod, napríklad:

- **Užívatelia neočakávajú príliš veľa príliš skoro.** Vo finále výkonnosť IT organizácie posudzujú užívatelia, takže je dôležité riadiť ich očakávania.
- **IT organizácia tým získava čas na zlepšenie v oblasti služieb.** Je to príležitosť pre IT organizácie, aby boli krok napred pred požiadavkami užívateľov. Organizácia si dokáže vytvoriť lepší obraz o nárokoch na zdroje spojených s plnením požiadaviek na dostupnosť, a to umožňuje lepšie plánovanie.
- **Umožňuje to menej náročné dohody.** Pokiaľ užívatelia vedia, že dohoda bude vylepšená neskôr, sú ochotnejší stanoviť realistický krátkodobý cieľ.

Nikdy sa nezaväzujte k niečomu, o čom viete, že nemôžete dosiahnuť. Dôležité je dohodnúť sa na cieli, ktorý môže byť dosiahnutý v krátkodobom horizonte, a stanoviť harmonogram pre dosiahnutie vyššej dostupnosti systému v budúcnosti. Vyskúšajte cieľ dostupnosti systému interne v rámci IT organizácie alebo v jednom malom oddelení. Potom, ako bolo demonštrované, že sa cieľ môže byť dosiahnutý, pokračuje zavádzanie nových štandardov úrovní služieb na celom zvyšku organizácie.

3.2.2 Identifikácia užívateľských požiadaviek na dostupnosť

Otázky na užívateľov, ktoré pomôžu identifikovať ich požiadavky na dostupnosť:

- Aké sú vaše plánované operácie? V akých hodinách dňa a v ktorých dňoch v týždni očakávate používanie systému alebo aplikácie?

  Odpovede na tieto otázky vám pomôžu určiť dobu, kedy musí byť systém alebo aplikácia k dispozícii. Väčšinou sa odpovede zhodujú s pravidelnou pracovnou dobou užívateľov. Napríklad, užívatelia väčšinou pracujú s aplikáciu od 8:00 do 17:00, od pondelka do piatku. Avšak niektorí užívatelia chcú mať prístup k systému aj po pracovnej dobe. V závislosti od počtu užívateľov, ktorí pristupujú k systému mimo pracovnej doby, môžete zahrnúť tieto časy do bežných prevádzkových hodín.

  Keď pristupujú k systému externí užívatelia alebo zákazníci, jeho prevádzková doba sa často rozširuje aj mimo bežnej pracovnej doby. To platí najmä pre on-line bankovníctvo, internetové služby, e-commerce systémy, a iné. Užívatelia týchto

systémov obvykle požadujú dostupnosť 24 hodín denne, 7 dní v týždni alebo čo najbližšie k tomuto stavu.

- Ako často môžete tolerovať výpadky systému v dobe, počas ktorej používate systém alebo aplikáciu?

  Vašou úlohou je pochopiť vplyv nedostupnosti systému na užívateľov v čase, keď je naplánovaný ako dostupný. Napríklad užívateľ môže povedať, že si môže dovoliť len dva výpadky za mesiac. Táto odpoveď tiež napovie, či môžete naplánovať výpadok v dobe, v ktorej by mal byť systém podľa dohody dostupný. Možno takto bude učinené kvôli údržbe, upgradom alebo iným údržbovým účelom. Napríklad systém, ktorý by mal byť on-line 24 hodín denne, 7 dní v týždni, stále vyžaduje plánovanú odstávku o polnoci na vykonanie úplnej zálohy.
- Ako dlho môže výpadok trvať v prípade, že k nemu dôjde?

  Táto otázka pomôže zistiť, ako dlho je užívateľ ochotný čakať na obnovenie systému pri výpadku alebo akú mieru výpadkov možno tolerovať bez vážneho ovplyvnenia podnikania. Napríklad, užívateľ môže povedať, že každý výpadok môže trvať maximálne tri hodiny. Často však môže užívateľ tolerovať dlhšie výpadky, ak sú naplánované.

3.3 Analýza súčasného stavu v malých a stredných firmách

3.3.1 Definícia malej a strednej firmy

Existuje mnoho definícií malej a strednej firmy (podľa počtu zamestnancov, obratu, atď.), pre túto prácu je však dôležitejšia veľkosť IT organizácie. Predovšetkým sa táto práca zameriava na dve špecifické cieľové skupiny:

- organizácie poskytujúce IT služby s obmedzenými finančnými prostriedkami,
- malé IT organizácie podporujúce malé a stredné firmy.

Veľkosť IT organizácie je v pomere k veľkosti celého podniku relatívny pojem (veľký podnik môže mať malé IT oddelenie a zase naopak). Veľkosť IT organizácie tiež určujú ukazovatele, ako napríklad: koeficient počtu IT zamestnancov v pomere k zákazníkom, rozsah outsourcingových aktivít, zložitosť IT prostredia a iné. [6]

Mnoho myšlienok a princípov v tejto práci má však široké uplatnenie bez ohľadu na to, či sa jedná o malú alebo veľkú organizáciu.

3.3.2 Analýza súčasného stavu

Malé a stredné organizácie v ČR, ktoré chcú začať s meraním a vykazovaním dostupnosti, však majú niektoré nedostatky v oblasti riadenia procesov, ktorých odstránenie je pre úspešnú implementáciu manažmentu dostupnosti veľmi dôležité. Tieto nedostatky sa dajú zhrnúť do nasledujúcich bodov:

- Pri implementácii ITSM procesov sa organizácie dostali maximálne po helpdesk. Evidujú incidenty, ale väčšinou ku koncovému zariadeniu, respektíve užívateľovi. Občas dokážu rozpoznať dĺžku incidentu od odhalenia po uzavretie incidentu. Kategorizácia incidentov je slabá, takisto sa nevedú priority incidentov. Pri evidovaní sa nepoužíva koncová služba, ale ide sa skôr po technologickej vetve (napr. nefunguje aplikácia XY, sieť, atď.)
- Neexistuje katalóg služieb, z čoho vyplýva, že organizácie nedokážu odvodzovať z akých komponentov, respektíve konfiguračných položiek (CI) sa daná služba skladá. Inak povedané, nedokážu presne určiť, čo umožňuje dodávku služby. Vyplývajú z toho nasledujúce problémy:
    1. Organizácie nedokážu zmerať dostupnosť koncovej služby, ale len jej jednotlivých komponentov;
    2. Organizácie nemôžu použiť metódy ako sú Analýza zlyhania služby (SFA) alebo Analýza dopadu zlyhania komponentu (CFIA), ktoré som opísal v teoretickej časti.
    3. Organizácie presne nevyčíslia náklady na službu. IT služba je tiež nákladová položka ako každá iná a sú s ňou spojené priame aj nepriame náklady.
- V rámci organizácie nikto nepopísal, prečo vlastne IT službu odoberá. Znamená to, že nikto vlastne nevypočítal návratnosť investície. S každou službou sú spojené určité náklady, ale rozhodujete sa pre ňu, pretože prináša určitú hodnotu, čo znamená, že by sa mala oplatiť. Čím viac se oplatí (čím väčšiu hodnotu prináša), tým väčšie investície si môžu organizácie dovoliť, pretože sa im vrátia. Iba pokiaľ by mali organizácie neobmedzené zdroje, nemuseli by sa zaoberať hľadaním vhodných investícií.
- Ďalším problémom sú neexistujúce SLA, pretože organizácie nevedia, ako ich majú zostaviť a čo v nich merať. Stáva sa aj to, že sa organizácie pokúšajú SLA zostaviť, ale s nezmyselnými metrikami.

- V organizáciách sa nerobí analýza funkčných dopadov (BIA, Business Impact Analysis). BIA by sa mala v organizácii vykonávať v prvej fáze procesu riadenia kontinuity činností. Jej cieľom je identifikácia procesov, stanovenie ich kritickosti a následne stanovenie možných dopadov v dôsledku nedostupnosti týchto procesov, napr. prerušenia produkcie alebo poskytovania služieb. Práve pomocou BIA potom organizácie dokážu identifikovať ich životne dôležité funkcie (VBF), inak povedané kritické podnikové procesy. [7]
- Taktiež častou chybou je, že v niektorých organizáciách bežia všetky služby v režime 24x7, čo je neefektívne. Znamená to, že náklady na prevádzku, respektíve na dostupnosť niektorých služieb sú neobhájiteľné. Sú proste príliš vysoké vzhľadom na nimi prinášanú hodnotu.

4 Návrh riešenia

4.1 Implementácia manažmentu dostupnosti

V skratke sa dá povedať, že manažment dostupnosti zahŕňa tieto štyri činnosti:

- Identifikácia kľúčových IT systémov a služieb v organizácii;
- Stanovenie požiadaviek na dostupnosť u týchto systémov a služieb;
- Zabezpečiť, aby tieto požiadavky boli splnené nákladovo efektívnym spôsobom;
- Reportovanie, monitorovanie a zlepšovanie dostupnosti IT.

4.1.1 Zásady implementácie ITIL

Niektoré zásady sú všeobecne platné, či už sa jedná o implementáciu ITIL ako celku alebo len jej jednotlivých častí a takisto sú platné, či je ITIL implementovaná v malej, strednej alebo veľkej firme.

1. Zásada:

Implementácia ITIL je celopodnikovým projektom strategického významu, a preto musí byť rozhodnutie o implementácii vykonané na úrovni najvyššieho podnikového vedenia a projekt musí mať z jeho strany viditeľnú podporu. [19]

2. Zásada:

Projekt sa dá rozdeliť do štyroch etáp, ktoré sa realizujú v tomto poradí:

1. **Získanie znalostí o ITIL:** Týka sa to spravidla manažérov, kľúčových zamestnancov podniku a členov implementačného tímu;
2. **Zhodnotenie súčasnej situácie:** Popis súčasného stavu a identifikácia oblastí, ktoré sú už pokryté;
3. **Naplánovanie a dosiahnutie cieľového stavu:** Vytvorenie projektového plánu a realizácia samotnej implementácie;
4. **Overenie dosiahnutia cieľu.** [19]

3. Zásada:

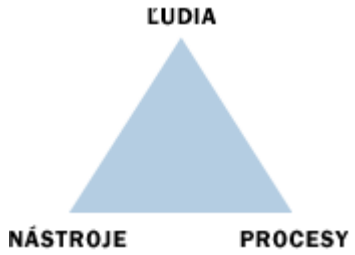
V priebehu celého projektu je žiaduce realizovať Awareness kampaň[14]. Pre úspech projektu má správne nastavené očakávanie zásadný význam, pretože pokiaľ sú očakávania

[14] Nástroj riadenia úrovne očakávania všetkých zainteresovaných strán. [19]

príliš vysoké, budú všetci z výsledku sklamaní bez ohľadu na to, že projekt skončí relatívne dobre. Na druhú stranu pokiaľ sú očakávania príliš nízke, nepodarí sa výstupy projektu uviesť do života, pretože všetci budú výsledkom zaskočení. [19]

4. Zásada:

Pri realizácii projektu je nutné udržať v rovnováhe trojuholník **ľudia - procesy - nástroje** (viď Obr. 4.1). Zamestnanci musia byť školení v ITIL a zaškolení na nové softwarové nástroje a pracovné procesy. Procesy musia byť zdokumentované a implementované (pracovné procedúry, náplne práce, organizačné smernice, atď.) Procesy ITSM musia byť podporované vhodnými softwarovými nástrojmi. Tieto nástroje musia byť implementované a spôsob ich používania musí byť popísaný v príslušnej dokumentácii. [19]



Obr. 4.1 Trojimperatív ľudia-procesy-nástroje (zdroj [19])

Nerešpektovanie tejto zásady má za následok nevyváženosť a plytvanie prostriedkami. Môže dôjsť k situáciám, že:

- sú implementované drahé softwarové nástroje, ale zamestnanci ich nevyužívajú správne, pretože nechápu súvislosti, lebo neabsolvovali školenie ITIL;
- pracovníci sú síce zaškolení a procesy sú správne vytvorené a implementované, ale nie sú podporované vhodnými softwarovými nástrojmi, takže dodržovanie vytvorených pracovných procedúr je komplikované a zamestnanci ich preto obchádzajú a nedodržiavajú;
- sú implementované vhodné softwarové nástroje a zamestnanci sú zaškolení tak na ich využívanie, ako aj majú znalosti o ITIL, ale procesy ITSM neboli vytvorené a implementované, v dôsledku čoho sa od používania novo-implementovaných nástrojov pozvoľna ustupuje a investície tak strácajú zmysel. [19]

4.1.2 Všeobecný postup implementácie manažmentu dostupnosti

Pri tvorbe tejto časti sú využité zdroje, ktoré sú v použitej literatúre uvedené pod označením [1] a [16].

Manažment dostupnosti môže byť implementovaný rôznymi spôsobmi. Pre mnoho organizácií môže byť mnou navrhnutá implementácia vhodná. Pre iné je zase vhodná implementácia takzvaného „veľkého tresku“. V praxi každá organizácia pristupuje k implementácii na základe svojich vlastných priorít. Zvážte nasledujúce kroky a potom použite vhodný model pre svoju vlastnú organizáciu.

Obr. 4.2 Kroky implementácie manažmentu dostupnosti

1. Určenie cieľov a rozsahu manažmentu dostupnosti.

ITIL V3 Best Practice doporučenia sú zložité a náročné na interpretáciu, ale predovšetkým v nich chýba konečné stanovisko o implementácii ITSM procesov. Mnohé IT organizácie sa následne púšťajú do implementácie ITIL bez solídnej predstavy o ich ceste k dosiahnutiu svojich cieľov, preto je tento krok veľmi dôležitý. [14]

2. Stanovenie jasnej definície slov:

- Dostupnosť (Availability)
- Spoľahlivosť (Reliability)
- Udržateľnosť (Maintainability)
- Servisovateľnosť, schopnosť poskytovať služby (Serviceability)
- Odolnosť (Resilience)

To je jeden z najzaujímavejších aspektov. Môže byť veľmi ťažké prinútiť všetkých, aby sa dohodli na definícii, a môže byť veľmi ťažké stanoviť správne pochopenie definície. Avšak, ak to urobíte poriadne, zvyšok procesu bude jednoduchší.

3. Počiatočné schválenie koncepcie.

Tento krok si vyžaduje vlastne to, čo je popísané už vyššie v prvej zásade implementácie ITIL. Je vhodné to spraviť formou písomného dokumentu, ktorý je schválený vedením.

4. Vytvorenie a definovanie rolí a zodpovedností za proces. Ustanovenie manažéra dostupnosti.

Pokiaľ začínate s manažmentom dostupnosti, toto je asi najdôležitejšia vec, ktorú musíte urobiť. Manažér dostupnosti vytvára jediný bod zodpovednosti za dostupnosť IT systémov a je šéfom plánovania dostupnosti v rámci organizácie.

Ak váš rozpočet alebo IT operácie neodôvodňujú ustanovenie špeciálnej osoby pre túto úlohu, nájdite vhodnú osobu v rámci organizácie a pridajte úlohu manažéra dostupnosti k individuálnym úlohám, ktoré vykonáva. Ak to urobíte, dbajte na to, aby pripadlo dostatok času z jej týždenného plánu na úlohu manažmentu dostupnosti a aby dôležitosť tejto úlohy bola jasne vysvetlená.

5. Zavedenie a definovanie rámca manažmentu dostupnosti a vzťahov s IT službami.

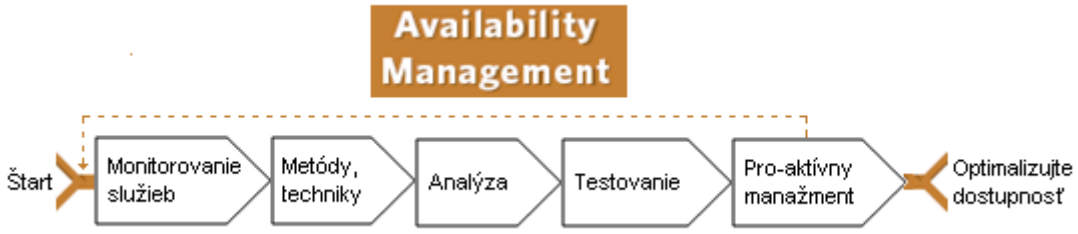
V prvom rade musíte identifikovať vaše kľúčové IT služby. V tomto kroku môžete definovať rozsah úlohy manažmentu dostupnosti katalogizáciou vašich kľúčových IT systémov a služieb. Nesnažte sa k tomu pristupovať z technologického pohľadu, otázkou „aké systémy máme“. Namiesto toho porozmýšľajte, aké kľúčové obchodné funkcie (VBF) vykonáva váš podnik, a z nich odvodíte kľúčové služby, ktoré sú potrebné na ich dodanie. Definujte vplyv každej obchodnej funkcie opísaním, aké dopady na obchod by nastali pri strate kľúčových služieb.

Povedzme, že sa zaoberáte priamymi obchodnými operáciami. Všetky obchody prechádzajú cez váš systém na spracovanie objednávok, takže si ho označíte ako kľúčovú

službu. Avšak pri pohľade na obchodnú funkciu zistíte, že päťdesiat percent nových objednávok prichádza cez e-mail, preto si aj váš e-mail systém pridáte na zoznam kľúčových služieb pre obchodnú funkciu.

6. Zavedenie procesu manažment dostupnosti.

Pri popisovaní tohto kroku som čerpal z materiálov, ktoré sú v použitej literatúre uvedené pod označením [14]. Pri zavedení tohto procesu si môžete pomôcť schémou, ktorú môžete vidieť na obrázku 4.2.



Obr. 4.3 Procesná mapa manažmentu dostupnosti (zdroj [14], autorsky upravený)

Táto schéma môže pomôcť manažérom pri vybudovaní základne, na ktorej môžu stavať pri napredovaní od nedostatočnej dostupnosti až k pro-aktívnemu riadeniu udržateľnej dostupnosti.

- **Monitorovanie služieb**

  Monitorovanie služieb je len jedna polovica z rovnice pre odvodzovanie meraní, ktoré tvoria základ pre riadenie. Správanie služby je výsledkom správania jej hlavných komponentov, takže komponenty by mali byť tiež sledované. Vzhľadom na rozmanitosť prvkov, ktoré tvoria služby v distribuovanom prostredí, to znamená, že manažéri sa stretnú s mnohými (a často odlišnými) zdrojmi údajov z monitorovania, ktoré budú musieť byť synchronizované, roztriedené a zosúladené alebo preložené.

  Táto činnosť musí poskytovať ostatným ITSM procesom informácie týkajúce sa skutočnej dostupnosti služieb a komponentov. Musí sa uskutočniť porovnanie medzi skutočnou dostupnosťou a dostupnosťou dohodnutou v SLA a OLA dohodách. Porovnanie vytvorí zoznam medzier, ktoré ukážu, kde je potrebné zlepšenie.

  Druhú polovicu rovnice tvoria prostriedky na údržbu dostupnosti a tiež prostriedky zlepšenia dostupnosti, ktoré sú rovnako monitorované pre porovnanie stupňa ich úspešnosti so záväzkami. Môže sa stať, že súčasné prostriedky nie sú dostatočné na splnenie SLA a budú sa musieť zmeniť. Ťažším rozhodnutím je zmeniť SLA dohody tak, aby boli prijateľnejšie pre existujúce prostriedky podpory. Nech sa rozhodnete pre ktorýkoľvek z týchto dvoch krokov, kľúčovým výkonnostným ukazovateľom (KPI)

procesu manažment dostupnosti bude percento služieb a komponentov infraštruktúry, ktorých dostupnosť je monitorovaná, spolu so schopnosťou odhaliť a identifikovať trendy v monitorovaných dátach.

- **Metódy, techniky**

  Monitorovanie tvorí základ pre riadiace metódy a techniky. Úsilie riadenia dotvára schopnosť konať na základe informácií, a to náležitým spôsobom.

  Konsolidácia širokej škály sledovaných informácií je dosiahnutá, keď sú dáta z rôznych sledovaní spojené do jedného modelu služby. Tento model služby najlepšie vytvoríte pomocou konfiguračnej databázy (CMDB). To isté platí pre architektúru zálohovania a zabezpečenia, pri prevencii chýb a zaisťovaní obnovy.

  Získavanie dôležitých informácií, pomocou potrebných kontrolných a detekčných techník, sa musí uplatňovať v takom rozsahu, ktorý je spoľahlivý, ale nebráni výkonu riadených služieb.

  Zabezpečte, aby boli dôležité informácie chápané z obchodného hľadiska, a ich integráciu, napríklad, do nástrojov na posúdenie manažmentu kapacít (momentálna výkonnosť kontra budúce požiadavky na výkonnosť) a manažmentu kontinuity IT služieb (momentálne požiadavky kontra riziká), ktoré by mali byť vyvinuté.

  Nakoniec by mali informácie, ktoré sú uvedené vyššie, vytvoriť stále virtuálne úložisko, organizované a fungujúce ako informačný systém manažmentu dostupnosti (AMIS).

- **Analýza**

  Prioritné analýzy informácií, ktoré ste získali vyššie, budú riešiť otázky, či je dostupnosť v ohrození, kde bola dostupnosť stratená a ako obnoviť dostupnosť. Ako súčasť efektívneho zachytenia hlavných faktorov týchto skúseností, manažéri budú potrebovať interpretovať odhalené a detekované výsledky s prahmi tolerancie, mapovaním k službám, a koeficientmi, ktoré stanovia, ako sú dôležité výsledky a tiež ako dôležité sú pre podnikanie. Tieto interpretácie by mali byť zavedené všade, kde je to možné, v rámci monitorovacích systémov, ale musí byť tiež súčasťou toho, ako AMIS zaznamenáva informácie. Real-time analýzy budú vychádzať z náležite pripravených monitoringov, zatiaľ čo post-facto analýza bude založená na údajoch obsiahnutých v AMIS. Z oboch prístupov by mali byť získané nasledujúce informácie: typ, počet a trvanie prerušení služby; degradácie služieb; príčiny prerušení a degradácií služieb; prerušenia a degradácie podľa typu služby, podľa typu komponentu, podľa SLA a OLA.

  Tieto kľúčové výkonnostné indikátory (KPI) budú informovať a potvrdzovať rozhodnutia o spôsoboch využitých na prevenciu, podporu a zlepšenie súčasného aj budúceho stavu.

- **Testovanie**

  Testovanie má dôležité miesto pred i po nasadení služby. Malo by overiť konfiguráciu služby a jej komponentov predtým, ako je služba nasadená. Potom by zase malo izolovať a potvrdiť kritického miesta alebo chyby, ktoré spôsobujú prerušenie a degradáciu dostupnosti.

  Pre manažment je opakovanie tejto činnosti veľmi dôležité. Testovanie pred nasadením novej služby potrebuje zistiť, či nasadenie bude mať vplyv na dostupnosť už implementovaných služieb a komponentov. Testovanie po nasadení by malo zas overiť, že aktuálne nároky na IT infraštruktúru nevyžadujú re-design, aby udržala krok s biznisom.

  Pravidelné testovanie je dôležité, iba občasné nestačí. Preto by mal byť zavedený testovací protokol na kontrolu priebežného prispôsobenia sa služieb s SLA. Objasní tiež rozdiel medzi neočakávanými výpadkami (ako sú incidenty) a plánovanými výpadkami, kedy je plánované, že dostupnosť bude nízka alebo žiadna.

- **Pro-aktívny manažment**

  Táto činnosť je síce posledná, ale jej dôsledkom býva opakovanie celého procesu. Prijímaním poznatkov a skúseností získaných z analýzy a testovania sú manažéri dostupnosti vyzbrojení vedomosťami potrebnými na vylepšenie alebo dokonca re-engineering existujúcich metód a techník používaných pre udržanie napredujúcej dostupnosti služieb. Prinesie to revíziu existujúcich plánov a návrhov a ich významu pri uspokojovaní biznisu. Dôsledkom tejto revízie budú zmeny pri vyhodnocovaní informácií získaných z monitorovania v manažmente kapacít a manažmente kontinuity IT služieb.

  V manažmente kapacít zistenia ovplyvnia identifikáciu zdrojov potrebných pre zabezpečenie dostupnosti. V manažmente kontinuity IT služieb bude stanovená relatívna kritickosť IT služieb a komponentov z hľadiska faktorov úspechu a rizík pre poskytovanie IT služieb podľa požiadaviek v dohodách.

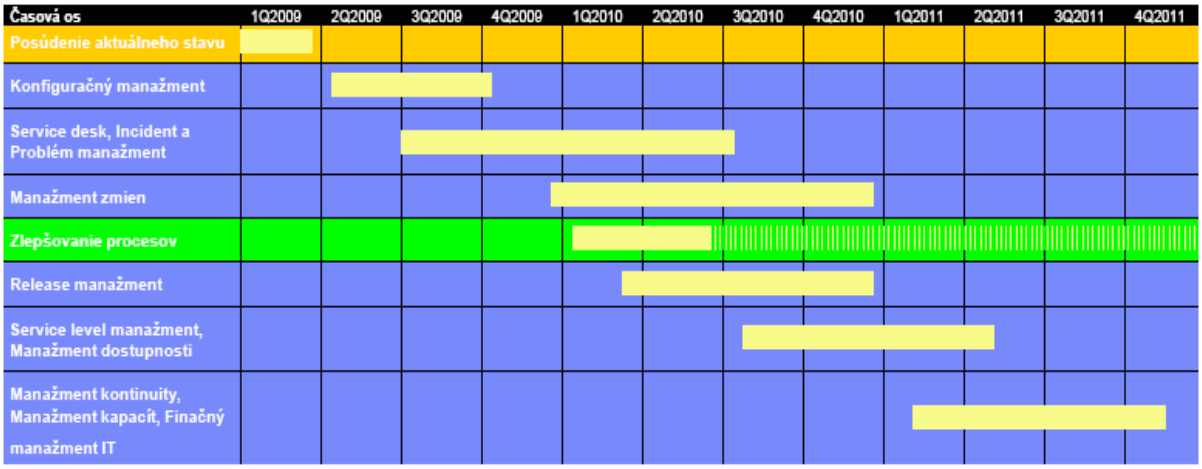
  Zabudovanie nízko-rizikovej flexibility do dostupnosti služby sa stáva dominantnou otázkou pro-aktívneho manažmentu dostupnosti.

7. Identifikácia vzťahov s ostatnými procesmi.

Ďalší z kľúčových krokov implementácie manažmentu dostupnosti. ITIL má veľa disciplín, z ktorých len jednou je manažment dostupnosti, ktorý je závislý na ostatných ITIL disciplínach, ako sú: Incident Management, Problem Management, Service Level

Management (manažment úrovní služieb), Configuration Management (konfiguračný manažment) a Change Management (manažment zmien).

Zo štúdie spoločnosti IBM Slovensko o postupe implementácie ITSM procesov jasne vyplýva, ako na seba nadväzuje implementácia jednotlivých procesov a ktoré procesy sú implementované pred manažmentom dostupnosti. Názorne je to ukázané na obrázku 4.2. Na obrázku môžete vidieť aj časovú os a odhad, kedy sa začne zlepšovanie procesov, a všimnite si, že v tomto prípade sú procesy manažment úrovní služieb a manažment dostupnosti implementované súčasne.



Obr. 4.4 Príklad prístupu k optimalizácii procesov u zákazníka (zdroj [15], autorsky upravený)

Pri vymedzovaní procesu manažment dostupnosti si musíte odpovedať na otázky, aké aktivity a aké informačné rozhrania tento proces má, aké vstupy a výstupy. Nezamotajte sa v snahe ísť príliš dopodrobna v informačných tokoch, ktoré idú do a z tohto procesu. V prípade procesu manažment dostupnosti môžeme vytvoriť jednoduchú tabuľku:

Proces	smer toku informácií	Proces	Informácie
Manažment dostupnosti	→	Manažment problémov	Reporty dostupnosti pre indikáciu súčasných a budúcich problémov.
Manažment problémov	→	Manažment dostupnosti	Hlásenie s dostupnosťou spojených problémov a známych chýb.
Manažment dostupnosti	→	Manažment zmien	Požiadavka na zmenu, Request for Change (RFC).
Manažment zmien	→	Manažment dostupnosti	Informácie o plánovaných zmenách, ako niektoré RFC môžu ovplyvniť dostupnosť.
Manažment dostupnosti	→	Manažment úrovní služieb	Reportovanie dostupnosti pre porovnanie plánovanej verzus aktuálnej.
Manažment úrovní služieb	→	Manažment dostupnosti	SLR, SLA, OLA, podporné kontrakty.
atď.			

Tab. 4.1 Tok informácií z a do procesu manažment dostupnosti (zdroj [1], autorsky upravená)

Podľa názoru odborníkov z praxe dosiahnete najlepšie výsledky vtedy, ak sú procesy incident a problém manažment vo vašej organizácii vyspelé a máte kompletnú a presnú konfiguračnú databázu (CMDB), z ktorej vychádzate.

IT služby sú poskytované IT infraštruktúrou. IT infraštruktúra vašej organizácie je definovaná a zdokumentovaná vo vašej konfiguračnej databáze (CMDB), ktorá vám poskytuje detailný prehľad o každej zložke, ktorá sa zúčastňuje na poskytovaní týchto kľúčových služieb. Bez týchto informácií bude takmer nemožné pre proces manažment dostupnosti uspieť. Takže ak nemáte žiadnu CMDB alebo máte CMDB, ktorej chýba presnosť a detailnosť, je najlepšie si jednu poriadnu urobiť pred tým, než sa pustíte do manažmentu dostupnosti.

Manažment dostupnosti je taktiež miesto, kde pomáhate nastaviť očakávania služby a ovplyvňujete ich vnímanie. Na dosiahnutie tohto cieľa manažment dostupnosti úzko spolupracuje s manažmentom úrovní služieb (SLM).

8. Zavedenie úrovne monitorovania.

Dostupnosť z pohľadu biznisu sa vzťahuje k službe a nie ku komponentom, ktoré tvoria službu. Meranie dostupnosti a zrovnanie skutočných úrovní dostupnosti s obchodnými požiadavkami je úplne zásadná činnosť pre každú z vašich kľúčových služieb.

9. Definovanie štandardov reportovania.

Reporting dostupnosti by mal vždy odrážať skutočný užívateľský komfort. V praxi to znamená, že pri reportingu sa musíte zamerať na službu ako celok, nie na komponenty, ktoré túto službu poskytujú. Pre užívateľov sú dôležité tie faktory, ktoré ovplyvňujú ich vnímanie dostupnosti:

- Doba trvania incidentov, ktoré vedú k nedostupnosti;
- Frekvencia, s ktorou sa tieto incidenty vyskytujú;
- Trvanie a frekvencia plánovanej údržby;
- Rozsah a možnosti dopadov.

V praxi vykonávajú ITSM nástroje takéto výpočty automaticky podľa potreby pre konfiguračné položky alebo pre služby na základe údajov o incidentoch a SLA patriacich ku konfiguračným položkám, respektíve k službám.

Reportovať priamo čísla prestojov je ďalší prístup, ktorý môžete využiť. Vaše reporty by však mali objasniť, ktorý bol nečakaný výpadok, v dôsledku chyby, a ktorý bol v dôsledku plánovanej údržby. Aj tento typ reportov ponúkajú niektoré ITSM nástroje.

Reporty pre vedenie podniku by mali obsahovať zhrnutia a analýzy, a nie surové dáta dostupnosti. Aby ste si urobili predstavu o údajoch, ktoré môžete použiť na vytvorenie reportu o dostupnosti pre vedenie podniku, ponúkam vám návod umiestnený v prílohách pod označením B.

Reporty vám povedia, kde treba dostupnosť zlepšiť, a pomocou svojich kľúčových informačných zdrojov, ako sú záznamy incidentov a problémov a vaša CMDB, môžete preskúmať, ktorá zložka alebo zložky sú zodpovedné za IT zlyhanie, hovorí sa tomu Single Point of Failure[15] (SPoF, jednotný zdroj zlyhania). Identifikácia alternatívnych komponentov pre SPoF je časť manažmentu dostupnosti, ktorá sa špecificky zameriava na redukciu zlyhaní. Vďaka tejto znalosti môžete potom vytvoriť prioritný akčný plán pre zlepšenie dostupnosti a úpravou IT infraštruktúry zaobstarať vyššiu úroveň spoľahlivosti.

10. Vytvorenie dokumentu obnovy dostupnosti.

Ak vychádzate z predpokladu, že chyby sa objavia, môžete to určitým spôsobom plánovať. Keď urobíte v správnom čase určité kroky, môžete negatívne vplyvy na biznis minimalizovať. Uistite sa, že sú plány obnovy dostupnosti riadne zdokumentované a pokiaľ je to možné, aj nacvičené a otestované. Tiež sa uistite, že sú napísané obnovovacie a reštart postupy, a že si zamestnanci podieľajúci sa na incident manažmente uvedomujú, že takéto postupy existujú, a vedia, kde ich nájsť. V praxi len málo ľudí, ktorí sú nablízku, keď sa niečo stane, ovláda postupy obnovy a reštartu, preto znovu pripomínam, ak môžete, cvičte a testujte tieto postupy. V prílohách pod označením C je umiestnená šablóna dokumentu obnovy dostupnosti.

11. Propagácia a marketing.

Nezabudnite, že kvalitnou a správnou implementáciou manažmentu dostupnosti dosiahnete určitú konkurenčnú výhodu, ktorú môžete využiť. Efektívne riadenie dostupnosti má vplyv na spokojnosť zákazníkov a rozhoduje o dobrom mene podniku na trhu.

[15] Každá konfiguračná položka, ktorá môže zapríčiniť incident, keď zlyhá, a pre ktorú nebolo implementované protiopatrenie. SPOF môže byť rovnako osoba alebo krok v procese alebo aktivite ako aj komponent IT infraštruktúry. [13]

4.2 Návrh riešenia pre malé a stredné firmy

Táto časť obsahuje doporučenia pre malé a stredné firmy ako konkrétne postupovať pri zavádzaní manažmentu dostupnosti, vzhľadom na problémy, ktoré sú popísané v analýze súčasného stavu.

4.2.1 Návrh postupu riešenia

Riešenie je rozdelené do troch fáz:

- **Inicializačné kroky:**
  1. Zostavte katalóg služieb. Tento katalóg bude obsahovať rozklad služieb na jednotlivé komponenty (CI, konfiguračná položka).
  2. Stanovte pre jednotlivé CI, aké služby podporujú a aký je dopad v prípade ich poruchy. Každej CI priraďte hodnotu kritickosti pre danú službu. Odporúčam použiť SPoF analýzu, ktorá je popísaná v teoretickej časti.
  3. Pri hlásení incidentov sa snažte nájsť CI, ktorá incident spôsobila. Na základe toho, ktoré služby podporuje, je možné povedať, že nefungovali všetky dané služby. Evidujte čas výpadku. Pre riadenie dostupnosti je nutné vedieť, kedy skutočne došlo k výpadku (incidentu), nie kedy bol odhalený.
  4. Evidujte všetky incidenty, aj tie, ktoré nespôsobili výpadok koncovej služby. Napríklad pri redundantných riešeniach výpadok jednej CI nemusí spôsobiť výpadok služby, ale je nutné evidovať incidenty, či už spôsobili výpadok koncovej služby, alebo nie. Evidencia je nutná pre výpočet spoľahlivosti, teda času medzi zlyhaniami (MTBF) a času na obnovu (MTTR) komponentov.
  5. Incidenty priraďte k problémom a podľa urgencie a dopadu im prideľte prioritu. Pomôže to nielen riadeniu užívateľskej podpory, ale tiež vám to napovie, ako naliehavý je ktorý problém, napríklad koľko závažných incidentov už spôsobil a bolo by dobré ho odstrániť. Toto všetko patrí do reaktívneho prístupu.
  6. Začnite merať. Na meranie dostupnosti existuje množstvo metrík (môžete sa inšpirovať nižšie v prípadovej štúdii).
- **Prvé výsledky:**
  1. Teraz by ste už mali byť schopný stanoviť dostupnosť koncovej služby, teda dôjsť k nejakému konkrétnemu číslu (môžete sa inšpirovať nižšie v prípadovej štúdii).

2. Tiež by ste mali byť schopný dojednať (v rámci prípravy SLA), že za daných podmienok ste schopný garantovať určitú úroveň dostupnosti IT služby (a budete už mať aj nejaké pádne argumenty). Stanovíte dostupnosť koncovej služby aj jej jednotlivých komponentov.
3. Pokiaľ zákazník s daným číslom nie je spokojný, stanovte príčiny tak nízkeho čísla a dajte mu priestor na predostretie jeho požiadaviek (SLR, požiadavky na úroveň služby).
4. Navrhnite odstránenie problémov. Rieši sa to pomocou manažmentu zmien, prípadne manažmentu dodávateľov, pokiaľ je problém na strane dodávateľa. Snažte se tiež, aby ste si neprivodili nové problémy.
5. Nájdite optimálny bod, kedy sa ešte do dostupnosti investovať oplatí, a kedy už nie. Je dôležité tento bod poznať najmä pri návrhu zlepšenia dostupnosti IT služby. Musíte porovnať náklady s prínosmi (môžete sa inšpirovať nižšie v prípadovej štúdii). Môže sa vám stať, že budete musieť upraviť očakávania (SLR).
6. Stále merajte.

- **Dostupnosť je nastavená:**

1. V tejto fáze už by mala byť dostupnosť dojednaná pre koncovú službu a formalizovaná v SLA. Dostupnosť je meraná a reportovaná a tieto informácie sú ukladané do AMIS (pokiaľ nejaký máte).
2. Akékoľvek zmeny komponentov (CI) sú posudzované (pomocou ich väzieb na iné CI), či ich prípadná zmena ovplyvní dostupnosť IT služieb dojednanú v SLA.
3. Pokiaľ sa objavia problémy, ktoré môžu ovplyvniť stanovenú dostupnosť, odstráňte ich príčiny (opäť pomocou manažmentu zmien) alebo inicializujte vyjednávanie o novej úrovni dostupnosti v SLA (toto zase rieši manažment úrovne služieb, SLM).
4. Sledujte a riaďte riziká (manažment kontinuity IT služieb).
5. Snažte se aj so súčasnými zdrojmi neustále zlepšovať dostupnosť, znižovať počet incidentov, dĺžku výpadkov, dobu na údržbu alebo odstávku (PSO).
6. Sledujte nové trendy a technológie (nižšie je uvedené niečo o virtualizácii).
7. Skúmajte vplyv kapacít a bezpečnosti na dostupnosť.
8. Testujte nové navrhnuté riešenia.

9. Stále merajte a vyhodnocujte.

4.2.2 Prípadová štúdia

Táto časť je vypracovaná pomocou materiálov, ktoré sú v použitej literatúre uvedené pod označením [11]. V tejto časti uvediem na príklade výpočet dostupnosti, odhad dostupnosti IT systému, porovnanie nákladov rôznych riešení dostupnosti a navrhnem spôsob vyčíslenia nákladov nedostupnosti.

Teraz vám predstavím jednoduchý matematický model na predpovedanie očakávanej dostupnosti u zložitých systémov. Pri riadení IT služieb je často nutné vytvoriť a zaviazať sa k dohodám o úrovni služieb (SLA). Ak však u systému nedôjde k analýze jednotných zdrojov zlyhania (SPoFA, je popísaná v teoretickej časti) a potom nedôjde k výpočtu dostupnosti systému, SLA budú chybné od samého začiatku. Aby to nebolo také jednoduché, existujú rôzne definície dostupnosti. Najčastejšie sa používajú tieto:

1. $$Dostupnosť = ((TST - DT) / TST) \quad (5)$$
(zdroj [16])

(TST - Total Service Time, celkový možný čas služby za obdobie, pre ktoré sa vykonáva výpočet, DT - Down Time, aktuálna doba trvania prestojov zaznamenaná za obdobie, pre ktoré sa vykonáva výpočet.) Tento vzorec na výpočet dostupnosti odporúča ITIL.

2. $$Dostupnosť = MTBF / (MTTR + MTBF) \quad (6)$$
(zdroj [11])

(MTBF - priemerný čas medzi zlyhaniami, MTTR - priemerný čas potrebný na obnovu) Toto je klasická definícia dostupnosti a často je požívaná výrobcami hardwaru, keď zverejňujú veličiny spojené s dostupnosťou pre určitý server.

3. $$Dostupnosť = (doba\ prevádzky + plánovaná\ údržba) / (neplánované\ prestoje + doba\ prevádzky + plánovaná\ údržba) \quad (7)$$
(zdroj [11])

Toto je ústredná IT veličina pre dostupnosť, kde podnik môže vyčleniť čas na plánované prestoje po pracovnej dobe. Tento model funguje pre niektoré typy systémov, napríklad file server, ktorý nie je potrebný v noci, ale nefunguje pre webové stránky, hoci mnohé webové firmy stále používajú tento typ výpočtu pre ich SLA.

4. *Dostupnosť = doba prevádzky / (doba prevádzky + prestoje)* (8)
(zdroj [11])

Táto veličina sa najlepšie aplikuje na systémy, ktoré sa používajú 24 hodín denne, 7 dní v týždni, ako napríklad webové stránky na elektronické obchodovanie.

Dostupnosť sa najčastejšie vyjadruje percentuálne. Pri návrhu vysokej dostupnosti sa často niektorý ľudia odvolávajú na štyri deviatky (99,99%) alebo päť deviatok (99,999%). Tabuľka 4.2 pre zjednodušenie udáva prípustný čas prestojov v rámci roka pre danú úroveň dostupnosti:

Dostupnosť	Prestoje (min)/rok	Prestoje (hod)/rok
95,000%	26298	438
98,000%	10519	175
98,500%	7889	131
99,000%	5260	88
99,500%	2630	44
99,900%	526	8,8
99,990%	52,6	0,88
99,999%	5,26	0,088

Tab. 4.2 Čas prestojov pre dané úrovne dostupnosti (zdroj[11])

Na základe tabuľky 4.2 môžete vidieť, že existuje veľký rozdiel medzi SLA určujúcimi dostupnosť na úrovni 99% (88 hodín prestojov ročne) a na úrovni 99,9% (8,8 hodín prestojov ročne). Však, nemôžeme si byť istý, aké sú očakávané prestoje systému. V najjednoduchšej forme sa očakávaná dostupnosť systému rovná očakávanej dostupnosti každého z komponentov v systéme, keď ich spolu vynásobíme. To znamená, že ak systém tvoria dva servery, a každý z nich mal očakávanú dostupnosť 99%, potom očakávaná dostupnosť systému by bola 99% * 99% = 98,01%. Chcem len upozorniť, že počítame očakávanú dostupnosť, to znamená budúce očakávania systému v rámci dlhšieho časového rámca, nie historické údaje o dostupnosti. Pre zvyšok tejto časti to platí tiež, no budem to vypúšťať kvôli stručnosti.

Tento model je síce jednoduchý, ale je veľmi užitočný, lebo názorne ukazuje to, že prestoje sú kumulatívna veličina. Inými slovami, ak očakávame, že každý komponent bude mať prestoje 88 hodín ročne a zlyhanie každého komponentu je zlyhaním celého systému, potom má systém očakávanú dobu prestojov povedzme 174 hodín. Určite sa opýtate, prečo nie 176 hodín. Pretože sa občas stáva, že dva komponenty sú mimo prevádzky v tom istom čase.

V reálnom svete systémy nie sú nikdy také jednoduché. Zvyčajne systém pozostáva z viacerých komponentov, niektoré s nadbytočnosťou, a každý z komponentov s rôznou úrovňou dostupnosti. Modelovanie týchto systémov vyžaduje o niečo zložitejšie vzorce, ale akonáhle je koncept pripravený, vlastný výpočet sa rýchlo vykoná v tabuľkovom editore. Pred tým než budem pokračovať, musím uviesť niekoľko zápisov, aby som zjednodušil zápis vzorcov:

1. Dostupnosť komponentu 1 = Dk_1
2. Dostupnosť komponentu 2 = Dk_2
3. Dostupnosť komponentu 3 = Dk_3
4. Dostupnosť komponentu n = Dk_n
5. Dostupnosť systému = D_s

Teraz bude nasledovať prvý vzorec. Ak sa systém skladá z *n* komponentov, kde každý z nich je jednotným zdrojom zlyhania, potom dostupnosť systému vypočítame takto:

$$Ds = Dk_1 * Dk_2 * Dk_3 * \dots Dk_n \quad (9)$$

(zdroj [11])

Predstavte si 24x7 webovú stránku elektronického obchodu s mnohými jednotnými zdrojmi zlyhania. Túto stránku by sme mohli namodelovať s nasledujúcimi ôsmymi komponentmi:

Komponent	Dostupnosť komponentu
Web	85,000%
Aplikácia	90,000%
Databáza	99,900%
DNS	98,000%
Firewall	85,000%
Switch	99,000%
Dátové centrum	99,990%
ISP	95,000%

Tab. 4.3 Komponenty e-comerce stránky a ich dostupnosť (zdroj[11])

Ak niektorý z týchto komponentov zlyhá, webová stránka spadne. Očakávaná dostupnosť stránky je 85%*90%*99,9%*98%*85%*99%*99,99%*95% = 59,87%. Všimnite si, že modelujeme každý komponent ako celok, nedívame sa na jeho súčasti. Mohli by sme rozložiť webovú službu do jednotlivých častí, ako je software (Apache), kód (webová stránka) a hardware (základná doska, pevné disky, atď.). Pre naše účely zložitosť nutne

nezlepší model, preto sa budeme zaoberať službou ako celkom. A aby som nezabudol, pre tento model použijeme štvrtú definíciu dostupnosti. Z hľadiska našich užívateľov neexistuje rozdiel, či je stránka nedostupná kvôli údržbe alebo kvôli zlyhaniu pevného disku.

Teraz sa pustíme do hľadania spôsobu, ako túto dostupnosť zvýšiť (predpokladám, že dostupnosť 59,78% nikoho neuspokojí). Dva zjavné ciele nášho snaženia na vylepšenie stability stránky budú webová služba a firewall. Otázkou je, aký vplyv na dostupnosť služby by malo pridanie ďalšieho webového serveru. To nás privádza k druhej rovnici. Ak systém tvoria nadbytočné komponenty, potom sa dostupnosť systému vypočíta ako:

$$Ds = Dk1 + ((1 - Dk1) * Dk2) \quad (10)$$

(zdroj [11])

Použime príklad webového serveru s dostupnosťou 85%, potom pridanie druhého serveru by viedlo k zvýšeniu dostupnosti na: 85% + (1-85%)*85% = 97,75%. Logika toho celého je v tom, že keď je prvý server nedostupný (15% celkového času), druhý server je stále dostupný na 85%. To sa môže a nemusí premietnuť do skutočnej dostupnosti. Napríklad, ak je webový server neustále nedostupný kvôli nastaveniu nového kódu, potom pridanie ďalšieho serveru by sa premietlo do zvýšenej dostupnosti, pretože kód by mohol byť nastavený na serveri, ktorý je nedostupný, zatiaľ čo ten druhý je dostupný. V tomto prípade by reálny nárast dostupnosti mohol byť vyšší ako 12,75%. Naopak ak je systém nedostupný kvôli chybám v programovom kóde, pridanie ďalšieho serveru by viedlo v niektorých prípadoch k zníženiu dostupnosti kvôli rozšíreniu chýb.

Dôležité je, že vo všeobecnosti, ak správne odhadnete dostupnosť komponentov, potom rovnica bude fungovať. Všimnite si, že rovnica funguje aj v prípade, že komponenty majú rôzniacu sa odhadovanú dostupnosť. Predpokladajme, že webový server má problémy s dostupnosťou kvôli nedostatočnému hardwarovému vybaveniu. Teraz predpokladajme, že druhý server, ktorý kúpime, bude mať dvojnásobnú kapacitu a určíme, že sama o sebe dostupnosť druhého serveru bude 90%, potom sa naša rovnica zmení na: 85% + (1-85%)*90% = 98.5%.

Predpokladajme, že sme pridali druhý webový server a druhý firewall, čím zvýšime dostupnosť každého z týchto dvoch komponentov systému na 97,75%. Teraz bude dostupnosť systému 97,75%*90%*99,9%*98%*97,75%*99%*99,99%*95% = 79,1%. Je to lepšie, ale stále nie dosť. Je ťažké dosiahnuť vyššiu úroveň dostupnosti, ak existujú jednotné zdroje zlyhania systému. Takže teraz predpokladajme, že pridáme nadbytočný (záložný) komponent pre všetky naše servery a vybavenie siete. Predpokladajme, že tiež pridáme ešte jeden ISP,

kvôli rôznorodosti nosičov, ale zostaneme stále v rámci jedného fyzického dátového centra. Naša rovnica dostupnosti teraz bude: 97,75%*99%*99,9999%*99,96%*97,75%*99,99% *99,99%*99,75% = 94,3%. Zlepšuje sa to. Odstránením jednotných zdrojov zlyhania sa dostupnosť systému zvýšila z 60% (3506 hodín prestojov ročne) na 94,3% (500 hodín prestojov ročne).

Predchádzajúca rovnica modelovala situáciu s pridaním jediného nadbytočného komponentu. Môžeme však mať viac než dva webové servery. V tom prípade musíme opakovať predchádzajúcu rovnicu niekoľkokrát, aby sme zistili účinok dodatočných komponentov, čo nás dovedie k tretej rovnici. Ak chceme vypočítať dostupnosť služby s *n* nadbytočnými komponentmi, vypočítame ju ako:

$$Ds = Dk_{(n-1)} + ((1 - Dk_{(n-1)}) * Dk_n) \quad (11)$$

(zdroj [11])

V našom príklade s webovou službou, pridanie tretieho serveru by zmenilo úroveň dostupnosti na 97,75% + (1-97,75%)*85% = 99,6625%. Pridanie štvrtého serveru by zvýšilo dostupnosť na 99,6625% + (1-99,6625%)*85% = 99,949%. Všimnite si, že miera návratnosti sa znižuje. Pridanie druhého serveru zvýšilo dostupnosť o 12,75%, pridanie tretieho serveru nám pridalo len 1,1925%, štvrtý server nám už len 0,2865%. A hoci by sme pridali aj ďalšie tri servery, čo je viac než potrebujeme na zvládnutie našej záťaže, ešte stále sme nedosiahli štyri deviatky dostupnosti. Navrhovanie vysoko dostupných systémov si vyžaduje, aby individuálne komponenty boli vysoko dostupné a pridanie nadbytočných komponentov. Ak by individuálny webový server v našom príklade mal dostupnosť 90%, namiesto 85%, potom by dostupnosť dvoch serverov bola 99% a troch 99,99%.

Druhá a tretia rovnica majú nedostatok v tom, že predpokladajú, že jediný komponent môže zvládnuť celú záťaž, a že toto zaťaženie systému je konštantné. Čo ak za normálnych okolností zvládne jeden server celú prácu, ale počas špičky, keď je zaťaženie najvyššie, potrebujeme tri servery? Potom by dostupnosť pre tri servery za normálnych okolností bola 99,775%, ale počas špičky by dostupnosť klesla späť na 85%. Počas špičky by zlyhanie jedného zo serverov spôsobilo stratu služby, takže klesneme späť k dostupnosti jediného kusu. Čo ak naša najvyššia záťaž vyžaduje dva servery? V tom prípade by dostupnosť počas špičky bola 97,75%. Ak najvyššie zaťaženie systému vyžaduje dva servery, a my máme tri, potom strata jedného z nich by nijako neovplyvnila fungovanie systému, preto je naša dostupnosť rovná situácii s dvoma servermi. Dôležitým konceptom tu je inverzný vzťah medzi záťažou a dostupnosťou.

Čo by už malo byť zjavné, je, že dosiahnutie naozaj vysokej úrovne dostupnosti (99,9% - 99,999%) je naozaj náročné a veľmi drahé. Jeden z najdrahších jednotných zdrojov zlyhania na odstránenie je dátové centrum. Vo väčšine prípadov toto zlepšenie zdvojnásobí náklady na infraštruktúru a náklady môžu byť dokonca vyššie než len dvakrát, pretože často je nutné investovať do technológií na udržiavanie serverov v každom dátovom centre v synchronizácii so všetkými ostatnými.

Napriek tomu, zvážme dopad pridania plne nadbytočného dátového centra. V našom príklade by dostupnosť nášho dátového centra s nadbytočnými servermi a ISP bola 94,3%. Pridanie druhého dátového centra s technológiou nutnou na ich fungovania v režime aktívny-aktívny (obe dátové centrá pracujú v tom istom čase) by zvýšilo dostupnosť na 94.3% + (1-94.3%)*94.3% = 99,675%. Pridanie druhého dátového centra by nám ušetrilo 471 hodín prestojov ročne.

V tomto príklade sme predpokladali, že každé dátové centrum bolo nezávislým systémom, preto zlyhanie služby v jednom dátovom centre by znamenalo zlyhanie celého systému v tomto dátovom centre. To nemusí byť vždy pravidlom. Napríklad pri správnom návrhu, webový server v jednom dátovom centre by sa mohol pripojiť k databázovému serveru v druhom dátovom centre. V tomto prípade by očakávaná dostupnosť systému bola vyššia než 99,675%. Ak by ste boli schopný navrhnúť webovú stránku tak, aby každá služba fungovala nezávisle na ďalších službách, potom by sa dostupnosť v našom príklade zvýšila z 99,675% na 99,888% (každá služba by mala 3 náhradné komponenty, okrem dátového centra, to by malo jeden náhradný komponent).

Je jednoduchšie tieto vzorce používať v tabuľkovom editore:

	A	B	C	D	E
1	Dostupnosť (%)	1 komponent	2 komponenty (1 dát. centrum)	3 komponenty (2 dát. centrá)	4 komponenty (2 dát. centrá)
2	Web	85,00%	=B2+((1-B2)*$B2)	=C2+((1-C2)*$B2)	=D2+((1-D2)*$B2)
3	Aplikácia	90,00%	=B3+((1-B3)*$B3)	=C3+((1-C3)*$B3)	=D3+((1-D3)*$B3)
4	Databáza	99,90%	=B4+((1-B4)*$B4)	=C4+((1-C4)*$B4)	=D4+((1-D4)*$B4)
5	DNS	98,00%	=B5+((1-B5)*$B5)	=C5+((1-C5)*$B5)	=D5+((1-D5)*$B5)
6	Firewall	85,00%	=B6+((1-B6)*$B6)	=C6+((1-C6)*$B6)	=D6+((1-D6)*$B6)
7	Switch	99,00%	=B7+((1-B7)*$B7)	=C7+((1-C7)*$B7)	=D7+((1-D7)*$B7)
8	Dátové	99,99%		=B8+((1-B8)*B8)	
9	ISP	95,00%	=B9+((1-B9)*$B9)	=C9+((1-C9)*$B9)	=D9+((1-D9)*$B9)
10	Dostupnosť systému (%)	=B2*B3*B4*B5*B6*B7*B8*B9	=C2*C3*C4*C5*C6*C7*D8*C9	=D2*D3*D4*D5*D6*D7*D8*D9	=E2*E3*E4*E5*E6*E7*D8*E9

Tab. 4.4 Výpočet vzorového príkladu v tabuľkovom editore (zdroj [11], autorsky upravená)

Aby ste si urobili lepší prehľad ponúkam vám aj výsledky:

Dostupnosť (%)	1 komponent	2 komponenty (1 dát. centrum)	3 komponenty (2 dát. centrá)	4 komponenty (2 dát. centrá)
Web	85,00%	97,75%	99,66%	99,95%
Aplikácia	90,00%	99,00%	99,90%	99,99%
Databáza	99,90%	100,00%	100,00%	100,00%
DNS	98,00%	99,96%	100,00%	100,00%
Firewall	85,00%	97,75%	99,66%	99,95%
Switch	99,00%	99,99%	100,00%	100,00%
Dátové centrum	99,99%		100,00%	
ISP	95,00%	99,75%	99,99%	100,00%
Dostupnosť systému (%)	59,87%	94,31%	99,21%	99,89%

Tab. 4.5 Výsledky výpočtov z tabuľky 4.4

Teraz, keď máme všetky základné koncepty hotové a tiež viete ako si vytvoriť súbor pre výpočet zmien týkajúcich sa našich predpokladov v tabuľkovom editore, môžete sa sústrediť na aplikáciu týchto teórií na vašu osobitú situáciu. Začnite rozložením systému, nech je to web stránka, účtovnícky program alebo file server, do jednotlivých komponentov služby. Pre každú službu určite minimálny počet jednotiek nutných na fungovanie systému a očakávanú dostupnosť jednotky.

Odhad dostupnosti môže byť výzvou. Jednou z metód by bolo pozrieť sa na historické dáta. Ak nemáte prístup k dobrým dátam, môžete vytvoriť váš odhad založený na štandardných operačných parametroch. Napríklad, ak zverejníte nový kód na webovom serveri dvakrát mesačne, a každé zverejnenie spôsobí dvojhodinový prestoj, to vyústi do 48 hodín prestojov ročne. Ak očakávate, že údržba operačného systému bude raz za štvrťrok s očakávaným prestojom 2 hodiny, ročne sa to bude rovnať 8 hodinám prestojov. Ak očakávate jedno zlyhanie hardwaru ročne a máte záruku ďalšieho obchodného dňa, to by znamenalo 41 hodín prestojov ročne (piatkové výpadky sú opravené v pondelok, výpadky v sobotu a v nedeľu v utorok). Pridaním týchto čísel dostaneme 48 + 8 + 41 = 98 hodín prestojov ročne alebo odhad dostupnosti na 98,882%.

S trochou námahy môžete pripraviť realistické odhady úrovne dostupnosti vášho systému. To je základ pre vytvorenie realistických a dosiahnuteľných SLA. Tieto vzorce môžu pomôcť IT pri vyjednávaní o SLA s podnikom a tiež pomôžu pri určení komparatívnych ROI (Return of Investment, návratnosť investícií) pre rozličné riešenia. Napríklad, povedzme, že chceme vybrať riešenie pre webový server a máme dve možnosti:

1. Prvá možnosť pozostáva zo štyroch serverov využívajúcich lacný hardware so žiadnou vnútornou nadbytočnosťou. Každý server stojí 3000€ a odhadnete dostupnosť každého zo serverov na 75%.
2. Druhá možnosť pozostáva z 2 serverov využívajúcich nákladný hardware s náhradnými pevnými diskami a dodávkami energie. Každý server stojí 20000€ a Odhadnete dostupnosť každého serveru na 99%.

Odhadnete náklady prestojov na 500€ za hodinu a očakávate, že tieto servery zvládnu celú záťaž vašej stránky len s jedným serverom ďalšie tri roky, a potom budú vymenené. Použijúc tieto údaje, riešenie 1. má očakávanú dostupnosť 99,6% pri nákladoch 12000€. Riešenie 2. má očakávanú dostupnosť 99,99% pri nákladoch 40000€. Riešenie 1. počíta s 34 hodinami prestojov ročne viac, čo je 102 hodín prestojov za tri roky viac ako riešenie 2. Za tri roky, náklady spojené s tými to extra prestojmi dosiahli 51000€. A tak vynaložením 28000€ popredu dosiahneme trojročnú návratnosť investície na úrovni 182%. Všimnite si, že tento model je len taký dobrý, ako sú vaše odhady. Ak by mali servery v druhom riešení dostupnosť len 95%, potom by ich celková dostupnosť bola 99,75%, čo by bolo len o 13 hodín prestojov ročne menej. V tomto prípade by sme ušetrili len 20000€ na prestojoch za tri roky pri investícii 28000€, preto by bolo lepšie riešenie 1.

Teraz by som vám ešte ponúkol pomôcku na lepší odhad nákladov na nedostupnosť, stačí doplniť tabuľku 4.6 a hodnoty doplniť do vzorca, ktorý je pod tabuľkou:

<table>
<tr><td colspan="4">Názov kľúčovej služby:</td></tr>
<tr><td colspan="4">Prestoje (v hodinách) {DT, Downtime}:</td></tr>
<tr><td>Postihnutí užívatelia v rámci organizácie {U, Users}</td><td></td><td>Priemerné celkové náklady (mzdy, režijné náklady) na jedného užívateľa {PU, per User}</td><td></td></tr>
<tr><td>Ušlé obchodné príjmy za hodinu {LBR, Lost Business Revenue}</td><td></td><td>Náklady na prácu nadčas {OT, Overtime}</td><td></td></tr>
<tr><td colspan="4">Ostatné náklady {S, Soundry cost}:</td></tr>
</table>

Tab. 4.6 Tabuľka na určenie nákladov nedostupnosti (zdroj **[**16])

$$Náklady\ nedostupnosti = (DT * U * PU) + (DT * LBR) + OT + S \quad (12)$$

(zdroj [16])

Navrhovanie a riadenie vysoko dostupných systémov je veľmi komplikovaná úloha, ale s niekoľkými jednoduchými vzorcami je možné porozumieť a predpokladať ich správanie na makro úrovni. Umožní vám to robiť lepšie rozhodnutia pri výbere rozličných riešení a tiež poskytovať realistickejšie odhady pri vyjednávaní SLA.

4.2.2.1 Využitie virtualizácie pri zlepšovaní dostupnosti

V dnešnej dobe sa o technológii virtualizácie veľa hovorí. Či už sa rozhodnete využiť Microsoft Hyper-V, VMware alebo dokonca Citrix Xen, virtualizácia vám pomôže maximalizovať prevádzkyschopnosť a dostupnosť dát a aplikácií. Pomocou virtualizácie serverov, môžete rozpoznať úspory nákladov ako alternatívu k drahému hardwarovému riešeniu.

Tradičné vysoko dostupné riešenia (využívajúce úplnú redundanciu) sú nákladné, ťažko sa zavádzajú a ťažko spravujú. S pomocou virtualizácie môžete zvýšiť základnú úroveň dostupnosti pre všetky vaše aplikácie a zabezpečiť, aby boli dohody o úrovni služieb (SLA) splnené. Virtualizácia vám poskytne úplne odstránenie plánovaných odstávok, predchádzanie neplánovaným prestojom a rýchle zotavenie sa z výpadkov, pretože:

- Eliminuje plánovanú odstávku pre bežnú údržbu;
- Zabezpečí vyššiu dostupnosť nezávisle na HW, operačnom systém a aplikáciách;
- Rýchlo sa obnovia systémy po serverových zlyhaniach a s automatickým reštartom.

Navyše zjednodušenie IT infraštruktúry a procesov bude mať za následok zníženie ďalších nákladov ušetrením miesta, energie a zdrojov.

4.3 Prínosy zavedenia manažmentu dostupnosti

Jednoducho povedané, výhodou implementácie manažmentu dostupnosti je, že IT organizácia pochopí potreby zákazníka a tieto potreby sú zadefinované a na základe zdrojov, které má k dispozícii, sa snaží poskytnúť optimálnu kvalitu.

Proces riadenia dostupnosti zabezpečí, že dostupnosť systémov a služieb je v súlade s meniacimi sa dohodnutými potrebami podniku. Dostupnosť a spoľahlivosť IT služieb môže priamo ovplyvniť spokojnosť zákazníkov a dobré meno podniku. Manažment dostupnosti zabezpečí, aby IT doručilo požadovanú úroveň dostupnosti IT služieb vyžadovanú podnikom na dosiahnutie podnikových cieľov a kvality služieb vyžadovanej zákazníkmi. Pokiaľ tomu tak nie je, poskytne vám argumenty, preč tomu tak nie je. Na dnešnom vysoko konkurenčnom

trhu je spokojnosť zákazníka so službami prvoradá. Nespokojnosť zákazníkov so službami a ich dostupnosťou môže byť rozhodujúca pri ich odchode ku konkurencii. [5]

Zavedením manažmentu dostupnosti dosiahnete prínosy pre podnikanie a pre IT organizáciu nasledujúcimi spôsobmi, ktoré podporujú hodnotu služieb:

- Pomáha pri konverzii inovatívnych myšlienok a koncepcií do služieb pre zákazníkov;
- Racionálne stanovuje riziká kontra obchodné príležitosti, ktoré reprezentujú dopyt užívateľov po službách;
- Poskytuje lepšiu kontrolu nainštalovaného HW a SW, ktorá povedie k zníženiu nákladov na licencovanie a údržbu;
- Systematicky presadzuje dodržiavanie dohodnutých úrovní služieb, ktoré udržujú očakávanú produktivitu podnikania;
- Manažér dostupnosti je zodpovedný za dostupnosť v rámci podniku, na rozdiel od stavu, keď je zodpovednosť rozptýlená medzi oddelenia a skupiny;
- Zbierajú a uchovávajú sa dáta, aby boli pre organizáciu zabezpečené zodpovedajúce úrovne dostupnosti;
- Sú zavedené merania a reporting, aby ste zistili, či je dodávaná požadovaná dostupnosť;
- Je kladený väčší dôraz na obchodné dopady nedostupnosti;
- Oveľa jednoduchšie vyčíslite náklady nedostupnosti;
- Je stanovený pro-aktívny rámec pre nápravu nedostupnosti, využitie plánov dostupnosti, SPoF analýzy a ďalšie techniky;

a mnohé ďalšie.

5 Záver

Cieľom mojej diplomovej práce bolo navrhnúť metodologickú príručku pre implementáciu manažmentu dostupnosti v malých a stredných firmách. Táto príručka mala vychádzať z ITIL.

Po naštudovaní kľúčových publikácií ITIL pre oblasť manažmentu dostupnosti som vypracoval teoretické východiská tohto procesu, ktoré rovnako ako ITIL popisujú ideálny stav, ktorý by mali organizácie dosiahnuť, ale neposkytuje návod ako manažment dostupnosti implementovať. V návrhovej časti som však popísal všeobecný postup, akým by mal byť podľa mňa tento proces implementovaný v malých a stredných firmách. Chcem zdôrazniť, že tento postup nie je záväzný, môže však slúžiť ako inšpirácia pre tých, ktorí sa rozhodnú manažment dostupnosti vo svojej organizácii implementovať.

Ďalej som v návrhovej časti popísal aj konkrétny postup, ako by mali malé a stredné firmy postupovať, keď chcú začať s manažmentom dostupnosti, ale musia najskôr odstrániť určité problémy, ktoré sú obvyklé a sú vymenované v analytickej časti. V závere návrhovej časti som sa v prípadovej štúdii snažil na príkladoch objasniť niektoré činnosti spojené s dostupnosťou, aby ste si o nich dokázali vytvoriť lepšiu predstavu.

Pri spracovaní danej témy som zistil, že manažment dostupnosti a tiež celá ITIL je veľmi komplexná záležitosť a nedá sa na jej implementáciu navrhnúť jeden konkrétny a všeobecne platný postup. Každá organizácia je iná a každá musí k implementácii pristúpiť svojím vlastným a pre ňu najvhodnejším spôsobom.

Hlavným cieľom manažmentu dostupnosti je zabezpečiť, aby bolo možné dodať IT služby s trvalou úrovňou dostupnosti nákladovo-efektívnym spôsobom, v súlade s obchodnými cieľmi organizácie. Manažment dostupnosti je dôležitou oblasťou ITIL procesov a je to proces, ktorý prináša merateľné prínosy. Táto diplomová práca pomáha lepšie porozumieť a podporuje schopnosť implementovať manažment dostupnosti v malých a stredných firmách.

Automatizácia ITSM môže prostredníctvom rôznych nástrojov a technológií pomôcť organizáciám znížiť množstvo zdrojov potrebných na dosiahnutie ITIL osvedčených postupov. Pomôže IT oddeleniam a organizáciám v zlepšovaní kvality ich služieb a zároveň im umožní sa pustiť do programu IT Service Excellence zameraného na podporu podnikateľského rastu.

Zoznam použitej literatúry

Tlačené zdroje:

[1] BLOKDIJK, G. a MENKEN, I. *Availability Management Best Practice Handbook: Building, Running and Managing Effective Availability Management-Ready to Use Supporting Documents Bringing Itil Theory Into Practice.* Emereo Pty Limited, 2008. 121 s. ISBN 192152393X.

[2] BLOKDIJK, G. a MENKEN, I. *Availability Management for It Services Best Practice Handbook - Proactively Manage and Maintain Service Levels to Meet Sla Expectations in Reliability.* Emereo Pty Limited, 2008. 116 s. ISBN 1921523530.

[3] CARTLIDGE, A. a kol. *An Introductory Overview of ITIL® V3*. The UK Chapter of the itSMF, 2007. 56 s. ISBN 0-9551245-8-1.

[4] OGC. *Best Practice for Service Delivery*. London: The Stationary Office, 2001. 378 s. ISBN 0-11-330017-4.

[5] OGC. *Service Design*. London: The Stationary Office, 2007. 334 s. ISBN 978-0-11-331047-0.

[6] SHARON, T. a MACFARLANE, I. *ITIL Small-scale Implementation.* London: The Stationary Office, 2006. 102 s. ISBN 0-11-330980-5.

Elektronické zdroje:

[7] *Analýza funkčných dopadov (Business Impact Analysis – BIA)* [online]. [cit. 2010-03-25]. Dostupný z WWW: < http://www.emm.sk/sk/produkty-a-sluzby/bezpecnost-is/bia >.

[8] Čo je ITIL® V3. *ITSM* [online]. [cit. 2010-03-03]. Dostupný z WWW: < http://www.itsm.sk/sk/ITIL/Co-je-ITIL-V3.alej >.

[9] Čo je to ITSM. *ITSM* [online]. [cit. 2010-02-23]. Dostupný z WWW: < http://www. itsm.sk/sk/ITSM/Co-je-to-ITSM.alej >.

[10] História a vývoj ITIL. *ITSM* [online]. [cit. 2010-02-23]. Dostupný z WWW: < http://www.itsm.sk/sk/ITIL/Historia-a-vyvoj-ITIL-.alej >.

[11] *In Search of Five 9s – Calculating Availability of Complex Systems* [online]. 2007. [cit. 2010-03-25]. Dostupný z WWW: < http://www.edgeblog.net/2007/in-search-of-five-9s/ >.

[12] *IT should establish realistic availability requirements* [online]. 2002. [cit. 2010-03-25]. Dostupný z WWW:
< http://articles.techrepublic.com.com/5100-10878_11-1060286.html?tag=rbxccnbtr1 >.

[13] itSMF Slovensko. *Slovník ITIL® v3, Anglicko-slovenský a slovensko-anglický slovník definícií, pojmov a skratiek* [online]. itSMF Slovensko, 2009. [cit. 2010-02-23]. Dostupný z WWW:
< http://www.itsmf.sk/files/documents/front/informacie/publikacie_itsmf/itil v3 glossary slovak-english v1.08 23.3.2009.pdf >.

[14] MALCOLM, R. *Availability Management: A CA Service Management Process Map* [online]. CA, 2009. [cit. 2010-03-25]. Dostupný z WWW:
< http://www.ca.com/files/ProcessMaps/availability-mgmt-process-map_222472.pdf >.

[15] PODHRADSKÝ, M. a KUBIŠ, D. *Ako pristupovať k optimalizácii IT procesov, dosiahnuť vyššiu efektivitu a celkové zníženie nákladov* [online]. IBM Corporation, 2009. [cit. 2010-04-02]. Dostupný z WWW:
< http://www-05.ibm.com/sk/events/ibmforum2009/pdf/aa_ako_pristupovat.pdf >.

[16] RITCHIE G. *Introducing ITIL® Availability Management* [online]. Serio Limited, 2007. [cit. 2010-02-23]. Dostupný z WWW:
< http://www.seriosoft.com/white_papers/serio_availability_management.pdf >.

[17] VRÁŽELOVÁ, L. Máte důvod přejít na ITIL v3? *IT Systems* [online]. 2009, č. 11, November [cit. 2010-02-17]. Dostupný z WWW: < http://www.systemonline.cz/sprava-it/mate-duvod-prejit-na-itil-v3.htm >. ISSN 1802-615X.

[18] VRÁŽELOVÁ, L. Seznamte se s novou verzí ITIL v3; Rozdíly mezi ITIL v2 a ITIL v3. *IT Systems* [online]. 2009, č. 11, November [cit. 2010-03-03]. Dostupný z WWW:
< http://www.systemonline.cz/sprava-it/seznamte-se-s-novou-verzi-itil-v3.htm >.
ISSN 1802-615X.

[19] Zásady implementácie disciplín ITSM. *ITSM* [online]. [cit. 2010-03-01]. Dostupný z WWW: < http://www.itsm.sk/sk/ITIL/Zasady-implementacie-disciplin-ITSM.alej >.

Zoznam skratiek

AMIS - Availability Management Information System

BCM - Business Continuity Management

CCTA - Central Computer and Telecommunications Agency

CFIA - Component Failure Impact Analysis

CI - Configuration Item

CMDB - Configuration Management Database

DT - Down Time

FTA - Fault Tree Analysis

HW - Hardware

ICT - Information and Communication Technology

IT - Information Technology

ITIL - IT Infrastructure Library

ITSCM - IT Service Continuity Management

ITSM - IT Service Management

itSMF - IT Service Management Forum

KPI - Key Performance Indicator

MTBF - Mean Time Between Failures

MTBSI - Mean Time Between Service Incidents

MTRS - Mean Time to Restore Service

OGC - Office of Government Commerce

OLA - Operational Level Agreement

PSO - Projected Service Outage

RFC - Request for Change

ROI - Return of Investment

SDP - Service Design Package

SFA - Service Failure Analysis

SKMS - Service Knowledge Management System

SLA - Service Level Agreement

SLP - Service Level Package

SLR - Service Level Requirement

SPoF - Single Point of Failure

SPoFA - Single Point of Failure Analysis

TST - Total Service Time

SW - Software

UC - Underpinning Contracts

VBF - Vital Business Function

Prohlášení o využití výsledků diplomové práce

Prohlašuji, že

- jsem byl seznámen s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, diplomovou práci užít (§ 35 odst. 3);
- souhlasím s tím, že diplomová práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího diplomové práce. Souhlasím s tím, že bibliografické údaje o diplomové práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, diplomovou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne 30. dubna 2010

……
Bc. Vladimír Spál

Adresa trvalého pobytu studenta:

Jaseňová 3216/11
010 07 Žilina
Slovenská republika

Zoznam príloh

A. Nové oblasti v ITIL V3

B. Šablóna správy o dostupnosti pre vedenie podniku

C. Dokument obnovenia dostupnosti

A. Nové oblasti v ITIL V3

Core ITIL v2 – All processes except Service Desk	Core ITIL v3 – Lifecycle approach	Comments
Service Desk	Service Desk	The focus remains the same
Incident Management	Incident Management Request Fulfilment	The addition of an optional request fulfilment process
Problem Management	Problem Management	Remains the same but is only covered as an overview
Change Management	Change Management	Slight changes in terminology i.e. CAB/EC – ECAB
Release Management	Release and Deployment Management	Release and deployment covered as an overview only but an introduction of the V model is best introduced here
Configuration Management	Service Asset and Configuration Management	Service Assets are included with Configuration. Covered as an overview
Service Level Management	Service Portfolio Management Service Level Management Supplier Management	Focus is on the Lifecycle approach and not the process of SLM. Included is Supplier Management and Service Portfolio Management
Financial Management for IT Services	Financial Management for IT Services	Main concepts are unchanged but the focus is more on economics and VOI
Capacity Management	Capacity Management	Capacity as an overview only there is the introduction of Demand Management at the Strategic level in terms of Value to the Customer
Availability Management	Availability Management Access Management	Availability as an overview and the introduction of Access Management
IT Service Continuity Management	IT Service Continuity Management	ITSCM as an overview supporting the Business Continuity
IT Security Management (EXIN only courses)	IT Security Management	The introduction of IT Security Management, (Only EXIN included this as a V2 process)

(zdroj: ILX Group plc.)

B. Šablóna správy o dostupnosti pre vedenie podniku

Názov správy

Analýza dostupnosti služby {*názov služby*}

Vypracované pre

{*pozície v podniku, pre ktoré je report určený*}

Obdobie, ktoré pokrýva správa

Máj 2009 {*napr.*}

Kľúčové štatistiky

{*Tu zhrniete biznis požiadavky na dostupnosť a dosiahnuté úspechy. Ak máte grafy a dáta z vášho ITSM systému, zvážte, či sa na ne budete odkazovať v prílohách. Táto časť by mala obsahovať napríklad:*

požadované hodiny prevádzky, cielenie dostupnosti

dosiahnutá aktuálna dostupnosť v percentách alebo prestoje v hodinách

počet incidentov, ktoré ovplyvnili dostupnosť, za mesiac

náklady nedostupnosti}

Trendy pre porovnanie

{*Použite štatistiky z predošlých mesiacov, aby ste objasnili, či sa trend zlepšuje alebo zhoršuje.*}

Zhrnutie obchodných dopadov

{*Tu môžete zhrnúť vplyvy na kľúčové obchodné úlohy. Rôzne časti podnikania budú ovplyvnené rôznymi spôsobmi, a preto by ste mali ku každej obchodnej úlohe pristupovať zvlášť.*}

{*referenčné číslo incidentu*}	{*obchodná úloha*}	{*zhrnutie obchodného dopadu*}	{*komentár obchodného zástupcu alebo manažéra*}

Analýza prípadov straty služby

{*Obsahuje informácie o nedostupnosti prípad od prípadu. Môže obsahovať:*

príčinu zlyhania

trvanie (buď stratené produkčné hodiny alebo čas začiatku a konca)

objektívne posúdenie, ako dobre bola chyba riešená, ako pracovali obnovovacie a reštart postupy

Ak máte plán dostupnosti, opíšte, ako ho táto situácia ovplyvní alebo ako sa na ňom odzrkadlila}

Budúce kroky a doporučenia

{*Siahnite po informáciách, ktoré ste doteraz získali, aby ste formulovali budúce kroky. Ak medzi ne patria kapitálové výdavky, ujasnite si, aký to bude mať vplyv na prestoje v budúcnosti a zahrňte tieto náklady do nákladov nedostupnosti.*}

(zdroj [16])

C. Dokument obnovenia dostupnosti

Prehľad pre exekutívu

{*Popíšte účel, rozsah a organizáciu dokumentu obnovenia dostupnosti.*}

Rozsah

{*Spočiatku nemôžu byť všetky IT služby zahrnuté v dokumente obnovenia dostupnosti. V tejto časti načrtnite, ktoré budú zahrnuté, a časový plán pre ďalšie služby, ktoré majú byť zahrnuté. Rozsah dokumentu obnovenia by mal určovať biznis, preto sa vzťahuje len na výber niekoľkých IT služieb poskytovaných IT oddelením, ktoré sú považované za zásadné pre podporu podnikových procesov. Poznámka: Tento dokument je treba odlišovať od IT plynulosti (continuity) obnovenia. Zahrňte do rozsahu rozdiel medzi kontinuitou a dostupnosťou IT služieb. Závisí to na tom, ako je služba definovaná v katalógu služieb. K zlepšeniu obnovenia vám poslúži analýza dopadu zlyhania komponentu (Component Failure Impact Analysis)*}

Prehľad dostupnosti služieb

{*Táto časť dokumentu obsahuje prehľad všetkých služieb uvedených v dokumente a príslušné informácie týkajúce sa obnovenia týchto služieb. Malo by to slúžiť ako kontrolný zoznam.*}

IT služba	Vlastník	Obchodný proces	Obchodný vlastníci	# SLA / odkaz na katalóg služieb	Pravdepodobnosť zlyhania	Čas obnovenia	Procedúra obnovenia	Podpora k dispozícii a otestovaná	Zachytené dáta
Služba A	J. Novák	fakturácie	K. Gott	SLA001			*{Zoznam príslušných procedúr. Toto si vyžaduje vstup z Incident a Problem manažmentu. }*		
Email	K. Novotný	komunikácia	H. Pospíšil	SLA243					
SAP	P. Muk	účtovníctvo a mzdy	J. Daniels	SLA123					

Služba A

Popis služby

{*V tejto časti stručne popíšte službu.*}

Pravdepodobnosť straty

{*V tejto časti popíšte pravdepodobnosť prerušenia služby a vplyv na biznis. Napríklad, bude sa strata služby opierať o kontrakt, v ktorom sú stanovené náklady s tým spojené? Ak stratíme túto službu, môžeme očakávať aj stratu zákazníkov, klientov, podielu na trhu? Definujte každú formu straty služby.*}

Zhoršenie služby

{*V tejto časti špecifikujte rýchlosť pre situáciu týkajúcu sa straty služby, ktorou asi dôjde k zhoršeniu celkového výkonu. Priraďte stupne od 1(ťažko rozpoznateľné) do 10 (rýchle tempo celkového zhoršenia), ktoré budú určovať, ako strata služby narastá na kritickosti.*}

Stupeň nárastu kritickosti	Z toho vyplývajúci obchodný dopad
9	Kompletná strata služby. Reputácia podniku v ohrození.
1	Menšie zhoršenie. Zákazníci si ho neuvedomujú.

Procedúry eskalácie

{*V tejto časti podrobne popíšte všetky procedúry eskalácie. Keď nastane chyba v službe, je dôležité poskytnúť stručný zoznam personálu, ktorý by mal byť kontaktovaný. To pomôže skrátiť dobu prerušenia služby.*}

Priorita	hierarchicky			funkčne			obchodne		
	meno	oddelenie	číslo	meno	oddelenie	číslo	meno	oddelenie	číslo
1									
2									
3									

Závislosť na zariadeniach

{*V tejto časti urobte zoznam tých zariadení, ktoré sú komponentmi danej služby. Keď tomuto porozumiete, pomôže vám to lepšie identifikovať miesto zlyhania, a tým skrátiť čas reakcie a obnovenia.*}

IT komponenty (konfiguračné položky (CI))					
# CI	Seriálové #	Názov CI	Typ	Sub - typ	Kritickosť
SER345	15434563	EMERO	HW	Server	Vysoká
RT5700	54444443	CISCO-002	HW	Router	Vysoká
RT45567	76547457	CISCO-001	HW	Router	Vysoká
MS001	N/A	MS Office	SW	Miscrosoft	Nízka

Podnikové potreby

{*Použite túto časť na popísanie všetkých informácií, ktoré potrebuje podnik, aby nimi bol zásobený, na pomoc pri riadení dopadov zlyhania na jeho procesy. Tiež to bude pomáhať pri stanovení správnych očakávaní a pri riadení problémov, ktoré môžu vyvstať následkom zlyhania.*}

IT potreby a zdrojové faktory

{*V tejto časti špecifikujte prepojenie zložitosti zariadení danej služby a úroveň schopností vyžadovanú od ľudí, ktoré dovolia danej službe, aby zostala v prevádzke v prípade zlyhania. Spíšte tiež všetky potrebné vzťahy s treťou stranou (predajcami).*}

Obnovovacie procedúry

{*V tejto časti by ste mali vytvoriť zoznam obnovovacích procedúr pre vyššie zaznamenané konfiguračné položky.*}

IT komponenty (konfiguračné položky (CI))						
# CI	Seriálové #	Názov CI	Typ	Sub - typ	Kritickosť	Obnovovacie procedúry
SER345	15434563	EMERO	HW	Server	Vysoká	
RT5700	54444443	CISCO-002	HW	Router	Vysoká	
RT45567	76547457	CISCO-001	HW	Router	Vysoká	
MS001	N/A	MS Office	SW	Miscrosoft	Nízka	

zdroj ([2])